ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Smart Cities: Privacy and Security

Αντώνης Παπακωνσταντίνου

Επιβλέπων Καθηγητής:
Στέφανος Γκρίτζαλης

ΠΕΙΡΑΙΑΣ

Νοέμβριος 2023

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Smart Cities: Privacy and Security

Αντώνης Παπακωνσταντίνου
Α.Μ.: E20124

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αποσκοπεί στην ανάλυση της ιδέας των Έξυπνων Πόλεων (Smart Cities) με έμφαση στην προστασία της ιδιωτικότητας και την ενίσχυση της ασφάλειας. Μελετούνται οι τεχνολογίες και οι πρακτικές που εφαρμόζονται σε Έξυπνες Πόλεις και προτείνονται μέτρα για τη διασφάλιση της ιδιωτικότητας των πολιτών για την αποτροπή πιθανών κινδύνων ασφαλείας. Η μεθοδολογία περιλαμβάνει τη συλλογή δεδομένων από επιστημονικές έρευνες και πειραματικές μελέτες, την ανάλυση τους και την ανάπτυξη προτάσεων πολιτικής. Τα κύρια αποτελέσματα περιλαμβάνουν συστάσεις για την αποτελεσματική εφαρμογή τεχνολογιών που σέβονται την ιδιωτικότητα και την ενίσχυση των μέτρων ασφαλείας σε Έξυπνες Πόλεις.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Τομέας Πληροφορικής , Τομέας Τεχνολογιών Επικοινωνίας

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Έξυπνες Πόλεις, Ιδιωτικότητα, Ασφάλεια, Τεχνολογία, Πληροφορική.

ABSTRACT

Internet of Things (IoT) is a system that integrates different devices and technologies, removing the necessity of human intervention. This enables the capacity of having smart (or smarter) cities around the world. By hosting different technologies and allowing interactions between them, the internet of things has spearheaded the development of smart city systems for sustainable living, increased comfort and productivity for citizens. The IoT for Smart Cities has many different domains and draws upon various underlying systems for its operation. In this paper, we provide a holistic coverage of the Internet of Things in Smart Cities. We start by discussing the fundamental components that make up the IoT based Smart City landscape followed by the technologies that enable these domains to exist in terms of architectures utilized, networking technologies used as well as the Artificial Algorithms deployed in IoT based Smart City systems. This is then followed up by a review of the most prevalent practices and applications in various Smart City domains. Lastly, the challenges that deployment of IoT systems for smart cities encounter along with mitigation measures.

SUBJECT AREA: IT Sector, Communication Technologies Sector

KEYWORDS: smart cities, internet of things (IoT) , sensing technologies, smart city challenges, privacy, security.

Η εργασία αυτή είναι αφιερωμένη στην οικογένεια μου και στη μνήμη της ξαδέρφης μου,

Ευθαλίας Κορδαμπάλου η οποία έφυγε πολύ νωρίς και άδικα από κοντά μας…

ΕΥΧΑΡΙΣΤΙΕΣ

Τις θερμότερες ευχαριστίες και από τη θέση αυτή οφείλω στον καθηγητή κ. Στέφανο Γκρίτζαλη για την επίβλεψη , σαφή καθοδήγησή του κατά την εκπόνηση της εργασίας , καθώς και για τις ουσιώδεις συζητήσεις μας.

Επιπλέον θα ήθελα να ευχαριστήσω τους φίλους μου και την οικογένεια μου για την οποιαδήποτε βοήθειά και συμβολή τους κατά την εκπόνηση της παρούσας πτυχιακής εργασίας μου.

Πειραιάς, Νοέμβριος 2023

ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενα

Πίνακας Περιεχομένων Εικόνων

Κεφάλαιο 1: Εισαγωγή

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) είναι ένας ευρύς όρος που αναφέρεται γενικά σε φυσικές συσκευές που συνδέονται με το διαδίκτυο και οι οποίες συλλέγουν, μοιράζονται ή χρησιμοποιούν δεδομένα. Αυτό περιλαμβάνει προσωπικές φορητές συσκευές, όπως ρολόγια, οικιακές συσκευές όπως τηλεοράσεις, τοστιέρες και ψυγεία, χαρακτηριστικά κτιρίων όπως ανελκυστήρες και φώτα, και αστικές υποδομές, όπως φωτεινούς σηματοδότες και κάδους απορριμμάτων.

Οι συσκευές IoT και τα δεδομένα που συλλέγουν μπορούν να προσφέρουν ευκολία, αποτελεσματικότητα και πληροφορίες ουσιαστικά σε κάθε πτυχή του κόσμου μας.

Για τον δημόσιο τομέα, το IoT παρέχει επί του παρόντος πολλά οφέλη και έχει τη δυνατότητα να δημιουργήσει ακόμη μεγαλύτερη αξία στο μέλλον. Οι έξυπνοι κάδοι μπορούν να ειδοποιούν τα απορριμματοφόρα όταν κοντεύουν να γεμίσουν, τα δικτυωμένα συστήματα έκδοσης εισιτηρίων μπορούν να βοηθήσουν στη βελτιστοποίηση των δημόσιων μεταφορών και τα αυτοματοποιημένα συστήματα παρακολούθησης μπορούν να απελευθερώσουν χρόνο για τους εκπαιδευτικούς στις τάξεις.

Οι καταναλωτές, οι κυβερνήσεις και οι επιχειρήσεις παντού χρησιμοποιούν ολοένα και περισσότερο συσκευές IoT και είναι ευρέως γνωστό ότι η χρήση του IoT θα συνεχίσει να επεκτείνεται με ταχείς ρυθμούς.

Ωστόσο, η «βιαστική είσοδος» στο IoT χωρίς την κατάλληλη προστασία της ιδιωτικής ζωής μπορεί να οδηγήσει σε επιβλαβείς και απροσδόκητες συνέπειες.

Καθώς το IoT αναπτύσσεται, η ποσότητα των δεδομένων που παράγει θα αυξάνεται παράλληλα με αυτήν. Αυτές οι μεγάλες συλλογές δεδομένων μπορούν, σε πολλές περιπτώσεις, να αποτελούν προσωπικές, υγειονομικές και ευαίσθητες πληροφορίες, εγείροντας πολλές προκλήσεις για την προστασία της ιδιωτικής ζωής.

Κεφάλαιο 2: Internet Of Things (IoT)

2.1 : Ορισμός IoT.

Ανάλογα με το με ποιον μιλάμε, το Διαδίκτυο των πραγμάτων (IoT) ορίζεται με διαφορετικούς τρόπους και περιλαμβάνει πολλές πτυχές της ζωής - από συνδεδεμένα σπίτια και πόλεις , συνδεδεμένα αυτοκίνητα και δρόμους έως και συσκευές που παρακολουθούν τη συμπεριφορά ενός ατόμου και χρησιμοποιούν τα δεδομένα που συλλέγονται για διάφορες υπηρεσίες. Κάποιοι αναφέρουν ένα τρισεκατομμύριο συσκευές συνδεδεμένες στο Διαδίκτυο μέχρι το 2025 και ορίζουν τα κινητά τηλέφωνα ως τα "μάτια και τα αυτιά" των εφαρμογών που συνδέουν όλα αυτά τα συνδεδεμένα «πράγματα».
Ανάλογα με το πλαίσιο, άλλοι δίνουν παραδείγματα που είναι λιγότερο επικεντρωμένα στα τηλέφωνα. Μιλάνε για μια κατηγορία συσκευών που δεν υπάρχουν σήμερα ή επισημαίνουν το έξυπνο σύστημα επαυξημένης πραγματικότητας της Google , με την χρήση των γυαλιών (Google's augmented-reality smart glasses) ως ένδειξη των πραγμάτων που πρόκειται να έρθουν.

Όλοι, ωστόσο, σκέφτονται το IoT ως δισεκατομμύρια συνδέσεις (ένα είδος "παγκόσμιου δικτύου" στο σύννεφο (cloud)) που θα περιλαμβάνει κάθε πτυχή της ζωής μας. Όλη αυτή η δημόσια συζήτηση υποδηλώνει ότι το IoT γίνεται επιτέλους ένα «καυτό» θέμα στα μέσα ενημέρωσης. Πολλά πρόσφατα άρθρα επισημαίνουν ότι το IoT είναι η αλληλεπίδραση και η ανταλλαγή δεδομένων μεταξύ μηχανών και αντικειμένων. Ως εκ τούτου, από τεχνολογική άποψη, το IoT ορίζεται ως ένα έξυπνο μηχάνημα που αλληλοεπιδράει και επικοινωνεί με άλλες μηχανές, αντικείμενα, και υποδομές, με αποτέλεσμα την παραγωγή όγκων δεδομένων και την επεξεργασία αυτών των δεδομένων σε χρήσιμες ενέργειες που μπορούν να "διοικήσουν και να ελέγξουν" τα πράγματα και να κάνουν τη ζωή πολύ πιο εύκολη για τον άνθρωπο.

Οι εκτιμήσεις για το μελλοντικό μέγεθος της αγοράς του IoT είναι πως θα καλύπτει ένα ευρύ φάσμα, αλλά οι περισσότεροι ειδικοί συμφωνούν ότι θα επισκιάσει κάθε άλλη αγορά. Στις ώριμες αγορές σήμερα, η απόλυτη, και πανταχού παρούσα καταναλωτική συσκευή είναι

το κινητό τηλέφωνο. Σκεφτείτε το δικό σας νοικοκυριό και μετρήστε τον αριθμό των κινητών τηλεφώνων που διαθέτετε σήμερα. Στη συνέχεια, μετρήστε τον αριθμό των παραθύρων, των πορτών, των ηλεκτρικών πριζών, των φώτων, των ηλεκτρονικών συσκευών και των μονάδων θέρμανσης και κλιματισμού που έχετε. Θα καταλάβετε γρήγορα γιατί η αγορά του IoT θα ξεπεράσει την αγορά των κινητών τηλεφώνων, τουλάχιστον στον δυτικό κόσμο.

2.2 : Τα χαρακτηριστικά του IoT

Τα θεμελιώδη χαρακτηριστικά του IoT είναι τα εξής:

1. **Διασυνδεσιμότητα (Interconnectivity)**: Όσον αφορά το IoT, όλα μπορούν να συνδέονται με την παγκόσμια πληροφόρηση και την επικοινωνιακή υποδομή.

2. **Things-related services**: Το IoT είναι σε θέση να παρέχει υπηρεσίες που σχετίζονται με τις συσκευές εντός των περιορισμών των πραγμάτων, όπως για παράδειγμα τη προστασία της ιδιωτικής ζωής και την σημασιολογική συνέπεια μεταξύ των φυσικών συσκευών και των αντίστοιχων εικονικών. Για να παρέχει τις παραπάνω υπηρεσίες, τόσο οι τεχνολογίες στον φυσικό κόσμο , όσο και στον κόσμο της πληροφορίας θα αλλάξουν.

3. **Ετερογένεια (Heterogeneity)**: Οι συσκευές στο IoT είναι ετερογενείς καθώς βασίζονται σε διαφορετικές πλατφόρμες και δίκτυα υλικού (software / hardware). Έτσι, μπορούν να αλληλοεπιδρούν με άλλες συσκευές ή πλατφόρμες υπηρεσιών μέσω διαφορετικών δικτύων.

4. <u>Δυναμικές αλλαγές (Dynamic changes):</u> Η κατάσταση των συσκευών αλλάζει δυναμικά, για παράδειγμα η αδράνεια είναι αυτοματοποιημένη, συνδέονται ή/και αποσυνδέονται στο δίκτυο βάσει της της ταχύτητας του δικτύου. Επιπλέον, ο αριθμός των συσκευών μπορεί να αλλάξει δυναμικά.

5. <u>Τεράστια κλίμακα (Enormous scale)</u>: Ο αριθμός των συσκευών που πρέπει να διαχειρίζονται και να επικοινωνούν μεταξύ τους θα είναι τουλάχιστον μια τάξη μεγέθους μεγαλύτερος από τις συσκευές που είναι ήδη συνδεδεμένες στο Διαδίκτυο.

Ακόμη πιο κρίσιμη θα είναι η διαχείριση των δεδομένων που δημιουργούνται και η ερμηνεία τους για σκοπούς εφαρμογής.
Αυτό σχετίζεται με τη σημασιολογία των δεδομένων, καθώς και με τον αποτελεσματικό χειρισμό τους.

6. <u>Ασφάλεια (Safety):</u> Καθώς κερδίζουμε οφέλη από το IoT, δεν πρέπει να ξεχνάμε την ασφάλεια. Ως δημιουργοί και ως αποδέκτες του IoT, εμείς πρέπει να σκεφτούμε και την ασφάλεια.
Αυτό περιλαμβάνει την ασφάλεια των προσωπικών μας δεδομένων και την ασφάλεια της σωματικής μας ευεξίας.
Ασφαλίζοντας τα δίκτυα και τα δεδομένα που διακινούνται σε όλες τις συσκευές θα δημιουργήσουμε ένα παράδειγμα ασφάλειας που θα κλιμακωθεί με τον καιρό.

7. <u>Συνδεσιμότητα (Connectivity)</u>: Η συνδεσιμότητα επιτρέπει την προσβασιμότητα στο δίκτυο. Η προσβασιμότητα είναι η είσοδος σε ένα δίκτυο ενώ η συμβατότητα παρέχει την κοινή ικανότητα κατανάλωσης και παραγωγής δεδομένων.

Ακολουθεί σχήμα με τις δυνατότητες του IoT.

Εικόνα 1 Διαδίκτυο των πραγμάτων: Ενεργοποιώντας την τεχνολογία

2.4: Η αρχιτεκτονική του IoT (IOT ARCHITECTURE)

Η αρχιτεκτονική του IOT αποτελείται από διαφορετικά επίπεδα τεχνολογιών τα οποία υποστηρίζουν την τεχνολογία IOT. Η αρχιτεκτονική χρησιμεύει για να δείξει πως οι διάφορες τεχνολογίες σχετίζονται μεταξύ τους και επικοινωνούν την επεκτασιμότητα και την διαμόρφωση της ανάπτυξης του IOT σε διαφορετικά σενάρια. Το σχήμα που ακολουθεί στο τέλος δείχνει την λεπτομερή αρχιτεκτονική του IOT.
Η λειτουργικότητα κάθε στρώματος περιγράφεται παρακάτω:

1. Έξυπνες συσκευές / το στρώμα του αισθητήρα (smart device / sensor layer):

Το χαμηλότερο επίπεδο αποτελείται από έξυπνα αντικείμενα ενσωματωμένα με αισθητήρες. Οι αισθητήρες επιτρέπουν τη διασύνδεση του φυσικού με τον ψηφιακό κόσμο , ο οποίος επιτρέπει την ύπαρξη πληροφοριών σε πραγματικό χρόνο οι οποίες συλλέγονται και υποβάλλονται σε επεξεργασία. Υπάρχουν διάφοροι τύποι αισθητήρων για διαφορετικούς σκοπούς. Οι αισθητήρες έχουν την ικανότητα να πάρουν μετρήσεις όπως θερμοκρασία, ποιότητα αέρα, ταχύτητα, υγρασία, πίεση, ροή, κίνηση , ηλεκτρισμός και άλλα.
Σε ορισμένες περιπτώσεις, οι αισθητήρες, μπορεί να έχουν κάποιο βαθμό μνήμης, επιτρέποντας να καταγράφουν ορισμένο αριθμό μετρήσεων. Ένας αισθητήρας μπορεί να μετρήσει κάποια φυσική ιδιότητα και να τη μετατρέψει σε σήμα , το οποίο , μπορεί να γίνει κατανοητό από ένα όργανο. Οι αισθητήρες ομαδοποιούνται ανάλογα με το σκοπό τους. Για παράδειγμα έχουμε περιβαλλοντικούς αισθητήρες, αισθητήρες σώματος, αισθητήρες οικιακών συσκευών και αισθητήρες οχημάτων. Οι περισσότεροι αισθητήρες απαιτούν συνδεσιμότητα με τις πύλες άλλων αισθητήρων. Αυτό μπορεί να γίνει με τη μορφή τοπικού δικτύου (LAN), όπως για παράδειγμα με συνδέσεις Ethernet και Wi-Fi. Για αισθητήρες που δεν απαιτούν συνδεσιμότητα με άλλους αισθητήρες , η συνδεσιμότητά τους με το backend, δηλαδή εξυπηρετητές/εφαρμογές , μπορεί να παρέχεται με τη χρήση Wide Area δικτύου (WAN), όπως το

GSM, το GPRS και το LTE. Αισθητήρες που χρησιμοποιούν συνδεσιμότητα χαμηλής ισχύος και χαμηλού ρυθμού δεδομένων, συνήθως σχηματίζουν δίκτυα κοινώς γνωστά , ως ασύρματα δίκτυα αισθητήρων (WSN). Τα WSN κερδίζουν ολοένα και μεγαλύτερη δημοτικότητα καθώς μπορούν να φιλοξενήσουν πολύ περισσότερους κόμβους αισθητήρων, διατηρώντας παράλληλα επαρκή διάρκεια ζωής της μπαταρίας και καλύπτοντας μεγάλες περιοχές.

2. <u>Πύλες και δίκτυα (Gateways and Networks)</u>:

Τεράστιος όγκος δεδομένων θα παραχθεί από αυτούς τους μικρούς αισθητήρες και αυτό απαιτεί μια ανθεκτική και υψηλής απόδοσης ενσύρματη ή ασύρματη υποδομή δικτύου ως μέσο μεταφοράς. Τα τρέχοντα δίκτυα, συχνά συνδεδεμένα με πολύ διαφορετικά πρωτόκολλα, έχουν χρησιμοποιηθεί για την υποστήριξη δικτύων μηχανής προς μηχανή (M2M) και τις εφαρμογές τους. Με τη ζήτηση που απαιτείται για την εξυπηρέτηση ενός ευρύτερου φάσματος υπηρεσιών και εφαρμογών IoT , όπως υπηρεσίες υψηλής ταχύτητας συναλλαγών, εφαρμογές ευαισθησίας περιβάλλοντος κ.λπ., απαιτούνται πολλαπλά δίκτυα με διάφορες τεχνολογίες και πρωτόκολλα πρόσβασης για να λειτουργούν μεταξύ τους σε μια ανομοιόμορφη διαμόρφωση. Αυτά τα δίκτυα μπορούν να είναι σε μορφή ιδιωτικών, δημόσιων ή υβριδικών μοντέλων και θα δημιουργούνται για να υποστηρίζουν τις απαιτήσεις επικοινωνίας για καθυστέρηση, εύρος ζώνης ή ασφάλεια.

.

3. <u>Στρώμα υπηρεσιών διαχείρισης (Management Service Layer)</u>:

Η υπηρεσία διαχείρισης στρωμάτων , διασφαλίζει την επεξεργασία πληροφοριών μέσω αναλύσεων, ελέγχων ασφαλείας, μοντελοποίησης διαδικασιών και διαχείρισης συσκευών.

Ένα από τα σημαντικότερα χαρακτηριστικά του επιπέδου υπηρεσιών διαχείρισης , είναι οι επιχειρησιακοί κανόνες και οι κανόνες διαδικασίας. Το IoT φέρνει τη σύνδεση και την αλληλεπίδραση αντικειμένων και συστημάτων μαζί, παρέχοντας πληροφορίες σε μορφή γεγονότων ή περιβαλλοντικών δεδομένων όπως η θερμοκρασία των εμπορευμάτων, η τρέχουσα τοποθεσία και τα δεδομένα κίνησης. Κάποια από αυτά τα γεγονότα απαιτούν φιλτράρισμα ή δρομολόγηση προς συστήματα επεξεργασίας , όπως η καταγραφή περιοδικών αισθητήριων δεδομένων, ενώ άλλα απαιτούν αντίδραση στις άμεσες καταστάσεις, όπως η αντίδραση σε έκτακτες καταστάσεις υγείας του ασθενή. Οι κανόνες υποστηρίζουν το σχηματισμό λογικής απόφασης και ενεργοποιούν διαδραστικές και αυτοματοποιημένες διαδικασίες για να επιτρέψουν ένα πιο (άμεσα) ανταποκρίσιμο σύστημα IoT.

Στον τομέα της αναλυτικής, χρησιμοποιούνται διάφορα εργαλεία ανάλυσης για να εξάγουν σχετικές πληροφορίες από μεγάλες ποσότητες ακατέργαστων δεδομένων και να επεξεργαστούν σε πολύ μεγαλύτερους ρυθμούς. Η αναλυτική , όπως η ανάλυση στη μνήμη , επιτρέπει την αποθήκευση μεγάλων όγκων δεδομένων στη μνήμη τυχαίας πρόσβασης (RAM) αντί να αποθηκεύονται σε φυσικούς δίσκους. Η ανάλυση στη μνήμη μειώνει τον χρόνο ερωτήματος δεδομένων και ενισχύει την ταχύτητα λήψης αποφάσεων. Η αναλυτική ροή είναι μια άλλη μορφή αναλυτικής όπου η ανάλυση των δεδομένων, θεωρούμενων ως δεδομένα εν κινήσει, πρέπει να πραγματοποιείται σε πραγματικό χρόνο, έτσι ώστε οι αποφάσεις να λαμβάνονται σε μερικά δευτερόλεπτα.

Η διαχείριση δεδομένων είναι η ικανότητα να διαχειριζόμαστε τη ροή των δεδομένων. Με τη διαχείριση δεδομένων στο επίπεδο υπηρεσίας

διαχείρισης, οι πληροφορίες μπορούν να προσπελαστούν, να ενσωματωθούν και να ελεγχθούν. Οι εφαρμογές σε υψηλότερα επίπεδα μπορούν να αποκρύψουν την ανάγκη επεξεργασίας περιττών δεδομένων και να μειώσουν τον κίνδυνο διαρροής προσωπικών πληροφοριών από την πηγή δεδομένων. Τεχνικές φιλτραρίσματος δεδομένων όπως η ανωνυμοποίηση δεδομένων, η ενσωμάτωση δεδομένων και ο συγχρονισμός δεδομένων χρησιμοποιούνται για να κρύψουν τις λεπτομέρειες των πληροφοριών, παρέχοντας μόνο τις απαραίτητες πληροφορίες που είναι χρήσιμες για τις σχετικές εφαρμογές. Με τη χρήση της αφαίρεσης δεδομένων, μπορούν να εξάγουν πληροφορίες για να παρέχουν μια κοινή επιχειρηματική αντίληψη των δεδομένων και έτσι να επιτευχθεί μεγαλύτερη ευελιξία και επαναχρησιμοποίηση σε διάφορους τομείς.

Η ασφάλεια πρέπει να επιβάλλεται σε ολόκληρη τη διάσταση της αρχιτεκτονικής του IoT, από το επίπεδο του έξυπνου αντικειμένου μέχρι το επίπεδο της εφαρμογής. Η ασφάλεια του συστήματος αποτρέπει την κακόβουλη εισβολή στο σύστημα και τις παραβιάσεις από μη εξουσιοδοτημένο προσωπικό, μειώνοντας έτσι τη δυνατότητα εμφάνισης κινδύνων.

4. <u>Στρώμα εφαρμογής (Application Layer)</u>:

Η εφαρμογή του Internet of Things καλύπτει "έξυπνους" χώρους/περιβάλλοντα σε τομείς όπως: Μεταφορές, Κτίρια, Πόλεις, Τρόπος ζωής, Λιανικό εμπόριο, Γεωργία, Εργοστάσια, Αλυσίδες εφοδιασμού, Έκτακτες ανάγκες, Υγεία, Πολιτισμός και τουρισμός, Περιβάλλον και Ενέργεια.

Προχωρώντας σε μία ανακεφαλαίωση έχουμε τα εξής.

Η αρχιτεκτονική του Διαδικτύου των Πραγμάτων (IoT) κατηγοριοποιείται ευρέως σε 4 επίπεδα.

1. Επίπεδο Αισθητήρων

Αυτό είναι το χαμηλότερο επίπεδο της αρχιτεκτονικής του IoT, το οποίο αποτελείται από δίκτυα αισθητήρων, ενσωματωμένα συστήματα, ετικέτες RFID και αναγνώστες ή άλλους αισθητήρες που διαφοροποιούνται ανάλογα το τομέα που χρησιμοποιούνται. Κάθε ένας από αυτούς τους αισθητήρες έχει αναγνώριση και αποθήκευση πληροφοριών (π.χ. ετικέτες RFID), συλλογή πληροφοριών (π.χ. δίκτυα αισθητήρων).

2. Επίπεδο Πρόσβασης και Δικτύου

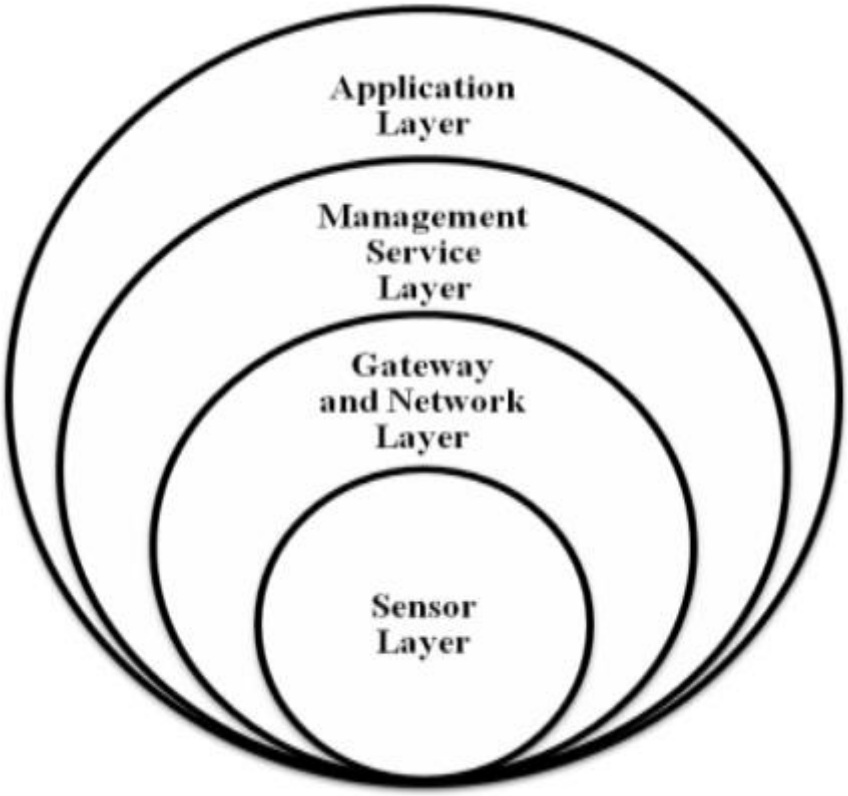
Αυτό το επίπεδο είναι υπεύθυνο για τη μεταφορά των πληροφοριών που συλλέγονται από τους αισθητήρες από το προηγούμενο επίπεδο. Θα πρέπει να υποστηρίζει ένα κλιμακούμενο, ευέλικτο, πρωτόκολλο καθολικών προτύπων για τη μεταφορά δεδομένων από ανομοιόμορφες συσκευές (διάφοροι τύποι κόμβων αισθητήρων). Αυτό το επίπεδο θα πρέπει να έχει υψηλή απόδοση και ανθεκτικό δίκτυο. Θα πρέπει επίσης να υποστηρίζει τις πολλαπλές οργανώσεις και να επικοινωνούν ανεξάρτητα.

3. Επίπεδο Υπηρεσιών Διαχείρισης

Αυτό το επίπεδο λειτουργεί ως διεπαφή μεταξύ του Επιπέδου Πρόσβασης και Δικτύου και του επιπέδου εφαρμογής. Είναι υπεύθυνο για τη διαχείριση των συσκευών και τη διαχείριση των πληροφοριών και υπεύθυνο για την καταγραφή μεγάλου όγκου δεδομένων και την εξαγωγή σχετικών πληροφοριών από τα αποθηκευμένα δεδομένα καθώς και από τα δεδομένα πραγματικού χρόνου. Πρέπει να εξασφαλίζεται η ασφάλεια και η ιδιωτικότητα των δεδομένων.

4. Επίπεδο Εφαρμογών

Αυτό είναι το υψηλότερο επίπεδο του IoT που παρέχει μια διεπαφή χρήστη για την πρόσβαση σε διάφορες εφαρμογές σε διάφορους χρήστες. Οι εφαρμογές μπορούν να χρησιμοποιηθούν σε διάφορους τομείς όπως οι μεταφορές, η υγεία, η γεωργία, οι αλυσίδες εφοδιασμού, η κυβέρνηση, το λιανικό εμπόριο.



Εικόνα 2 Τα στρώματα της αρχιτεκτονικής του Διαδικτύου των Πραγμάτων

2.5: Εφαρμογές του IoT

2.5.1: Εφαρμογή στον τομέα της γεωργίας:

2.5.1.1: Έξυπνη γεωργία:

Οι αισθητήρες συλλέγουν και αναλύουν πληροφορίες περιβάλλοντος, όπως η τρέχουσα θερμοκρασία, οι συνθήκες υγρασίας του εδάφους, η υγρασία των φύλλων και η ηλιακή ακτινοβολία, ενημερώνοντας στη συνέχεια τον ιδιοκτήτη/αγρότη σχετικά με τις ανάγκες σε νερό, φυτοφάρμακα, λίπασμα ή θεραπεία για τα μολυσμένα φυτά.

2.5.2: Εφαρμογή στον τομέα της υγείας:

2.5.2.1: Παρακολούθηση υγείας:

Το Διαδίκτυο των Πραγμάτων (IoT) χρησιμοποιείται στον τομέα της υγείας για τη βελτίωση της ποιότητας της ανθρώπινης ζωής, υποστηρίζοντας βασικές εργασίες που πρέπει να εκτελούν οι άνθρωποι μέσω εφαρμογών. Οι αισθητήρες μπορούν να τοποθετηθούν σε εξοπλισμό παρακολούθησης της υγείας που χρησιμοποιούν οι ασθενείς. Οι πληροφορίες που συλλέγονται από αυτούς τους αισθητήρες είναι διαθέσιμες στο Διαδίκτυο σε γιατρούς, μέλη της οικογένειας και άλλα ενδιαφερόμενα μέρη προκειμένου να βελτιωθεί η ανταπόκριση και η θεραπεία. Επιπλέον, οι συσκευές IoT μπορούν να χρησιμοποιηθούν για την παρακολούθηση των τρεχουσών φαρμάκων ενός ασθενούς και για την αξιολόγηση του κινδύνου νέων φαρμάκων ως προς αλλεργικές αντιδράσεις και επιπλοκές. Με τη χρήση αισθητήρων και της παραπάνω τεχνολογίας μπορούμε να παρακολουθούμε τη θερμοκρασία του σώματος, τον παλμό της καρδιάς, την πίεση του αίματος κλπ. Σε περίπτωση έκτακτης ανάγκης, το άτομο και ο προσωπικός του γιατρός θα ενημερωθούν με όλα τα δεδομένα που συλλέγονται από τους αισθητήρες. Αυτό το σύστημα θα είναι

πολύ χρήσιμο για ηλικιωμένους και άτομα με αναπηρίες που ζουν ανεξάρτητα.

2.5.2.2: Φαρμακευτικά προϊόντα:

Η ασφάλεια των φαρμακευτικών προϊόντων είναι πρωταρχικής σημασίας για την προστασία της υγείας των ασθενών. Η προσάρτηση έξυπνων ετικετών στα φάρμακα και η παρακολούθηση της κατάστασής τους με αισθητήρες έχει οφέλη όπως η διατήρηση των συνθηκών αποθήκευσης, η λήξη των φαρμάκων, πράγμα που θα αποτρέψει τη μεταφορά ληγμένων φαρμάκων στους ασθενείς.

2.5.3: Εφαρμογή στον τομέα του περιβάλλοντος:

2.5.3.1: Έξυπνη Παρακολούθηση ποιότητα αέρα:

Με την ενσωμάτωση αισθητήρων συλλέγονται πληροφορίες περιβαλλοντικού πλαισίου, όπως η ποσότητα μονοξειδίου του άνθρακα (CO), διοξειδίου του αζώτου (NO2) στον αέρα, τα επίπεδα ήχου, θερμοκρασίας, επιπέδων υγρασίας στο περιβάλλον. Αυτό παρέχει συνεχή πληροφορία σχετικά με το περιβάλλον, το οποίο βοηθάει να ληφθούν προφυλάξεις σε περίπτωση που υπερβαίνει το φυσιολογικό επίπεδο.

2.5.3.2: Έξυπνη Παρακολούθηση ποιότητα νερού:

Αισθητήρες μπορούν να ανιχνεύουν τη ποιότητα του νερού, τη ροή του νερού, τη ταχύτητα, τη θερμοκρασία, τη ρύπανση του νερού, τα περιεχόμενα του νερού. Αυτό βοηθάει στην πραγματική ανάλυση και διαχείριση των υδατικών πόρων που είναι διαθέσιμοι για χρήση.

2.5.3.3: Έξυπνη διαχείριση απορριμμάτων:

Οι ενσωματωμένοι αισθητήρες στο δοχείο λυμάτων βοηθούν στον έλεγχο της υπερχείλισης των αποβλήτων που ρέουν μέσα, παρέχοντας συνεχώς πληροφορίες σχετικά με το επίπεδο των αποθηκευμένων λυμάτων. Με βάση αυτά τα δεδομένα, το προσωπικό συντήρησης μπορεί να προγραμματίσει τη διαδικασία επεξεργασίας του νερού για να αποφευχθεί η υπερχείλιση των λυμάτων.

2.5.4: Εφαρμογή στον τομέα των πόλεων:

2.5.4.1: Έξυπνο σπίτι / Έξυπνη κοινωνία:

Στις μέρες μας, σπίτια και γραφεία χρησιμοποιούν τεχνολογίες IoT. Διάφορες ηλεκτρονικές συσκευές και συστήματα HVAC, όπως φώτα, ανεμιστήρες, φούρνοι μικροκυμάτων, ψυγεία, θερμαντήρες και κλιματιστικά, ενσωματώνονται με αισθητήρες για να χρησιμοποιούν την ενέργεια επαρκώς, να παρακολουθούν και να ελέγχουν την ποσότητα θέρμανσης, ψύξης και το επίπεδο του φωτός.Τα φώτα των δωματίων αντιλαμβάνονται την παρουσία ανθρώπων και ανάβουν όταν μπαίνετε, όταν εντοπίζεται φωτιά ή καπνός στο σπίτι, τα ασύρματα αισθητήρια καπνού και μονοξειδίου του άνθρακα εκπέμπουν σειρήνες κινδύνου και ειδοποιούν επίσης μέσω τηλεφώνου ή email και προσφέρουν περισσότερη άνεση στη ζωή, με αποτέλεσμα τη μείωση του κόστους και την αύξηση της εξοικονόμησης ενέργειας.

Το IoT μπορεί να χρησιμοποιηθεί για τον απομακρυσμένο έλεγχο και προγραμματισμό των συσκευών στο σπίτι σας. Μπορεί να είναι χρήσιμο στον εντοπισμό και την αποτροπή κλοπών.

2.5.4.2: Έξυπνη κυκλοφορία:

Προς το παρόν, η διαχείριση της κυκλοφορίας είναι ένα μεγαλύτερο πρόβλημα στις μεγάλες πόλεις. Η διαχείρισή τους με το χέρι έχει γίνει σχεδόν αδύνατη. Αυτό το πρόβλημα μπορεί να ξεπεραστεί με την εφαρμογή του Διαδικτύου των πραγμάτων (IoT) για τη διαχείριση της κυκλοφορίας. Αυτή η έξυπνη παρακολούθηση της κυκλοφορίας χρησιμοποιεί αισθητήρες για τη συλλογή ακατέργαστων δεδομένων κυκλοφορίας, τα οποία παρέχουν ενημέρωση κυκλοφορίας στον οδηγό, βοηθώντας τον να πάρει την απόφαση για τη διαδρομή του. Αυτό επίσης βοηθάει τον χρήστη να κλείσει ένα ταξί χωρίς τηλεφωνική κλήση ή να εντοπίσει τη θέση επιβίβασης και επίσης να εμφανίζει τα ταξί που είναι κοντά αλλά και την κίνησή τους σε πραγματικό χρόνο.

2.5.4.3: Έξυπνο πάρκινγκ:

Θα τοποθετηθούν αισθητήρες στις θέσεις στάθμευσης για να γνωρίζουν εάν η θέση στάθμευσης είναι διαθέσιμη ή όχι. Οι οδηγοί παρκάρουν το όχημά τους κοιτάζοντας την εφαρμογή που παρέχει λεπτομέρειες για τις πλησιέστερες διαθέσιμες θέσεις στάθμευσης, το κόστος στάθμευσης βασισμένο στα δεδομένα που συλλέγονται και αναλύονται από τους έξυπνους αισθητήρες, οι οποίοι τους βοηθούν να εξοικονομήσουν χρόνο και καύσιμα.

2.5.4.4: Έξυπνος φωτισμός πόλεων:

Αισθητήρες που μπορούν να αναλύσουν την ώρα, την εποχή, τις καιρικές συνθήκες, θα ενσωματωθούν στους δρόμους φωτισμού που αυτόματα ανάβουν ή θα σβήνουν και θα ρυθμίζουν τα επίπεδα φωτισμού ατομικά ή για ομάδα φώτων βάσει των διαδικασιών που θα αναπτυχθούν γύρω από αυτό.

2.6: Βασικά πλεονεκτήματα του IoT

Αυτή η τεχνολογία έχει πολλές εφαρμογές σε διάφορους τομείς.
Παρακάτω παρουσιάζονται μερικοί πιθανοί τομείς όπου μπορούμε να εκμεταλλευτούμε τη δύναμη του Διαδικτύου των Πραγμάτων (IoT) για να λύσουμε καθημερινά προβλήματα. Ωστόσο, μπορεί να χρησιμοποιηθεί σε πολλές περισσότερες χρήσεις.

2.6.1: Επικοινωνία

Στο Διαδίκτυο των Πραγμάτων υπάρχει επικοινωνία μεταξύ συσκευών, στην οποία οι φυσικές συσκευές είναι σε θέση να παραμένουν συνδεδεμένες και, συνεπώς, η συνολική επικοινωνία είναι διαθέσιμη με λιγότερες ανεπάρκειες και μεγαλύτερη ποιότητα.

2.6.2: Αυτοματισμοί και έλεγχοι

Χωρίς ανθρώπινη εμπλοκή, οι μηχανές αυτοματοποιούν και ελέγχουν μεγάλες ποσότητες πληροφοριών, προκειμένου να παράγουν ταχύτερα και έγκαιρα αποτελέσματα.

2.6.3: Εξοικονόμηση χρημάτων και χρόνου μέσω της παρακολούθησης

Το IoT χρησιμοποιεί έξυπνους αισθητήρες για την παρακολούθηση διαφόρων πτυχών της καθημερινής μας ζωής για διάφορες εφαρμογές, οι οποίες εξοικονομούν χρήματα και χρόνο.

2.6.4: Καλύτερη ποιότητα ζωής

Οι εφαρμογές βασισμένες στο Διαδίκτυο των Πραγμάτων (IoT) αυξάνουν την άνεση και βελτιώνουν τη διαχείριση στην καθημερινή μας ζωή, βελτιώνοντας έτσι την ποιότητα ζωής.

2.6.5: Νέες επιχειρηματικές ευκαιρίες

Δημιουργεί νέες επιχειρήσεις για την τεχνολογία του Διαδικτύου των Πραγμάτων, και έτσι αυξάνει την οικονομική ανάπτυξη και τις νέες θέσεις εργασίας.

2.6.6: Καλύτερο περιβάλλον

Σώζει φυσικούς πόρους και δένδρα και βοηθά στη δημιουργία ενός έξυπνου, πιο πράσινου και βιώσιμου πλανήτη.

2.7: Μειονεκτήματα του IoT

2.7.1: Συμβατότητα

Παρόλο που οι συσκευές από διαφορετικούς κατασκευαστές είναι συνδεδεμένες στο Διαδίκτυο των Πραγμάτων (IoT), προς το παρόν, δεν υπάρχει διεθνές πρότυπο συμβατότητας.

2.7.2: Πολυπλοκότητα

Το Διαδίκτυο των Πραγμάτων είναι ένα ποικίλο και πολύπλοκο δίκτυο. Οποιαδήποτε αστοχία ή σφάλματα στο λογισμικό ή το υλικό θα έχουν σοβαρές συνέπειες. Ακόμα και η διακοπή ρεύματος μπορεί να προκαλέσει πολλές δυσκολίες.

2.7.3: Ιδιωτικότητα / Ασφάλεια

Το Διαδίκτυο των Πραγμάτων (IoT) περιλαμβάνει τη συμμετοχή πολλών συσκευών και τεχνολογιών, και πολλές εταιρείες θα το παρακολουθούν. Καθώς πολλά δεδομένα που σχετίζονται με το περιβάλλον θα μεταδίδονται από τους έξυπνους αισθητήρες, υπάρχει υψηλός κίνδυνος απώλειας προσωπικών δεδομένων.

2.7.4: Μείωση απλού προσωπικού / Κλείνουν θέσεις εργασίας

Με τον ερχομό της τεχνολογίας, οι καθημερινές δραστηριότητες αυτοματοποιούνται με τη χρήση του Διαδικτύου των Πραγμάτων με λιγότερη ανθρώπινη παρέμβαση, η οποία από τη σειρά της

προκαλεί λιγότερες ανάγκες για χρήση ανθρώπινου δυναμικού. Αυτό προκαλεί πρόβλημα ανεργίας στην κοινωνία.

2.7.5: Η τεχνολογία παίρνει τον έλεγχο της ζωής

Οι ζωές μας θα ελέγχονται όλο και περισσότερο από την τεχνολογία και θα εξαρτώνται από αυτήν. Η νεότερη γενιά είναι ήδη εθισμένη στην τεχνολογία για κάθε μικρή λεπτομέρεια. Με το Διαδίκτυο των Πραγμάτων, αυτή η εξάρτηση θα διαδοθεί σε διάφορες γενιές και στις καθημερινές ρουτίνες των χρηστών. Πρέπει να αποφασίσουμε πόσο από τις καθημερινές μας ζωές είμαστε διατεθειμένοι να μηχανοποιήσουμε και να ελέγχεται από την τεχνολογία.

Εικόνα 3 Πλεονεκτήματα και μειονεκτήματα του Διαδικτύου των Πραγμάτων

Κεφάλαιο 3: Smart Cities

3.1 : Τι είναι η smart city;

Όπως παρατήρησαν , σε μία έρευνα η οποία έγινε από το Εθνικό Εργαστήριο Brookhaven το 2000:
Μια εικόνα της πόλης του μέλλοντος έχει παρουσιαστεί – μια πόλη , η οποία , που στηρίζεται στην ενσωμάτωση της επιστήμης και της τεχνολογίας μέσω των πληροφοριακών συστημάτων. Ένα μέλλον που θα απαιτήσει μια επανεκτίμηση των σχέσεων μεταξύ κυβέρνησης, διαχειριστών πόλεων, επιχειρήσεων, ακαδημαϊκής κοινότητας και ερευνητικής κοινότητας. Ο τίτλος αυτής της – νέας- πόλης , είναι Έξυπνη Πόλη. Αυτή η παρατήρηση θέτει τις βάσεις για τη μελέτη μας για τις έξυπνες πόλεις. Ο ορισμός μας δεν αποκλίνει πολύ από αυτόν του Hall. Μια έξυπνη πόλη χρησιμοποιεί τεχνολογίες πληροφορικής και επικοινωνιών για να αυξήσει τη λειτουργικότητα και αποτελεσματικότητα της, να μοιραστεί πληροφορίες με το κοινό και να βελτιώσει την ποιότητα των υπηρεσιών. Για να επιτύχουν αυτούς τους στόχους, οι πόλεις χρησιμοποιούν τεχνολογία σε διάφορα μέρη της υποδομής της πόλης. Αυτά τα τεχνολογικά συστήματα θα χρησιμοποιήσουν αισθητήρες για τη συλλογή δεδομένων σχετικά με το περιβάλλον και τις λειτουργίες της πόλης, κεντρική και κατανεμημένη ή ενσωματωμένη υπολογιστική ισχύ για την επεξεργασία αυτών των δεδομένων και συστήματα για το χειρισμό της αστικής υποδομής και την προσαρμογή των λειτουργιών της πόλης. Σε αυτήν την έννοια, η έξυπνη πόλη μετατρέπει την πόλη σε ένα μεγάλο τεχνολογικό σύστημα που "αισθάνεται, σκέφτεται και ενεργεί".
Ωστόσο, η ευρεία εφαρμογή τεχνολογίας εισάγει προκλήσεις στη μεταφορά κινδύνου, την ευθύνη, την προστασία των πολιτών, τη διαχείριση δεδομένων και τη συγκατάθεση των πολιτών.

3.2 : Η ιστορία των smart cities

Οι πόλεις βρίσκονται υπό αυξανόμενη πίεση να αντιμετωπίσουν ένα σύνολο πολύπλοκων προκλήσεων. Μερικές από αυτές είναι: Πρόκληση

ποιότητας του αέρα, κλιματικής αλλαγής (τόσο οι επιπτώσεις, όπως η αύξηση των θερμοκρασιών και ο κίνδυνος πλημμύρας, όσο και η επιτακτική ανάγκη για άμεση δράση), συμφόρησης κυκλοφορίας, προσιτότητας της στέγασης, δημόσιας υγείας, κοινωνικής ανισότητας κ.α. Μία από αυτές τις προκλήσεις είναι οι ελαττωματικές υποδομές που δεν ενσωματώνουν πιθανώς μετασχηματιστικές τεχνολογίες και πρακτικές, ορισμένες από τις οποίες αυξάνουν δραματικά την αποδοτικότητα των πόρων, επιτρέπουν την ομαλή ροή της κυκλοφορίας, βελτιώνουν τη δημόσια υγεία και ενισχύουν την ανθεκτικότητα.

Οι Έξυπνες Πόλεις περιέχουν υποδομές που διαποτίζονται με ΤΠΕ (Τεχνολογίες Πληροφορίας και Επικοινωνιών) προκειμένου να διευκολύνουν την παρακολούθηση και διαχείριση υπηρεσιών όπως η μεταφορά, η χρήση ενέργειας και η ποιότητα του νερού. Οι περισσότερες ανεπτυγμένες πόλεις περιέχουν ήδη στοιχεία της Έξυπνης Πόλης, όπως αισθητήρες που παρακολουθούν την ποιότητα του αέρα, την κυκλοφορία, το πάρκινγκ ή τα φώτα του δρόμου. Νεότερες και πιο συζητημένες διαστάσεις, ωστόσο, αφορούν τη χρήση του δημόσιου χώρου, το προβληματικό προαίσθημα της αστυνόμευσης ή τον έλεγχο του πλήθους. Ο δυναμικός διάλογος γύρω από την προσέγγιση της έξυπνης πόλης θέτει σημαντικά ερωτήματα διακυβέρνησης σχετικά με τους διαφορετικούς τρόπους με τους οποίους η τεχνολογία μπορεί τόσο να προωθήσει όσο και να εμποδίσει αποτελεσματικές προσεγγίσεις για τη δημόσια υγεία και τη βιωσιμότητα. Με άλλα λόγια, μπορούν τα πλούσια δεδομένα που παράγονται από τους πολίτες στους αστικούς χώρους, καθώς και οι τεχνολογίες που παράγουν και καταναλώνουν αυτά τα δεδομένα, να διακυβερνηθούν με έναν τρόπο που είναι διαφανής και επικεντρωμένος στον πολίτη; Όπως και σε κάθε πολύπλοκο σύστημα, υπάρχουν απρόσμενες συνέπειες και πιθανώς κρυμμένοι κύκλοι ανατροφοδότησης. Μπορεί να είναι περιβαλλοντικά βιώσιμη μία πόλη, αλλά όχι προσιτή. Αυτή η εργασία εξερευνά αυτά τα ερωτηματικά για να αποκαλύψει όχι μόνο τα δυνητικά οφέλη μιας έξυπνης πόλης για την επιτάχυνση των μεταβάσεων προς τη βιωσιμότητα, αλλά και τις σημαντικές προκλήσεις διακυβέρνησης που προκύπτουν καθώς επιχειρούμε να σχεδιάσουμε κοινότητες που είναι υγιείς και δίκαιες.

3.3 : Η αρχιτεκτονική των smart cities

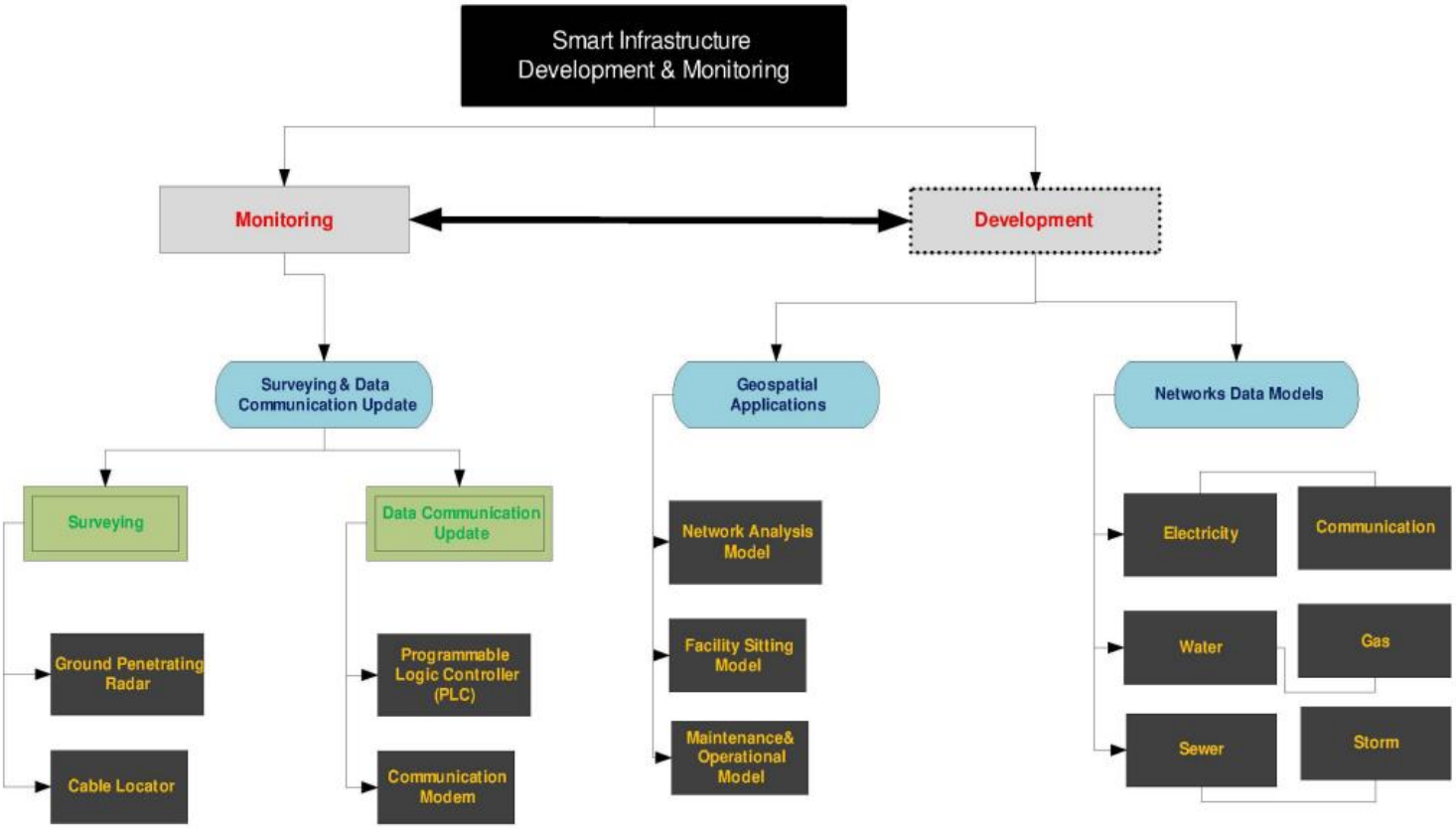
Η υποδομή έχει διάφορες σημασίες ανάλογα με τον περίγυρο που χρησιμοποιείται. Σε όρους λειτουργικότητας και χρηστικότητας, η υποδομή αναπαριστά τα δίκτυα υπόγειων και επιφανειακών καλωδίων και σωλήνων, μαζί με όλα τα σχετικά στοιχεία. Ενώ οι πολιτικοί μηχανικοί , ασχολούνται με άλλες λειτουργίες υπηρεσιών στο αστικό περιβάλλον, όπως τα οδικά δίκτυα, γέφυρες, σιδηροδρομικοί σταθμοί και σταθμοί λεωφορείων, σχολεία, νοσοκομεία, πανεπιστήμια και άλλες δημόσιες υπηρεσίες.

Τα συμβατικά δίκτυα υποδομής αποτελούνται από κύρια και σημαντικά στοιχεία που συνδέονται με σωλήνες ή τροφοδοτικά. Ορίζεται ότι το μεγαλύτερο μέρος αυτών των στοιχείων δεν επικοινωνούν μεταξύ τους και έχουν πολύ περιορισμένες λειτουργικότητες ελέγχου και παρακολούθησης. Το κύριο σκεπτικό για την ίδρυση των ψηφιακών δικτύων υποδομής είναι να διανείμει ένα επαρκές αριθμό αισθητήρων που να ανταποκρίνονται στο απαιτούμενο επίπεδο συνδεσιμότητας και ελέγχου των ενεργητικών. Ο Thomas (2001) πρότεινε το έξυπνο συμβατικό δίκτυο υποδομής για το σύστημα παρατήρησης του ωκεανού. Το συζητούμενο σκεπτικό ασχολείται με τις πλατφόρμες παρατήρησης δικτύου και τους αισθητήρες που αναπτύσσονται σε ένα ευρύ γεωγραφικό εύρος, κατανεμημένοι σε όλο τον ωκεανό. Το δίκτυο χρησιμοποιεί μια ποικιλία συνδέσεων επικοινωνίας, συμπεριλαμβανομένων οπτικών ινών, μικροκυμάτων, πακέτων ραδιοφώνου, δορυφορικών και ακουστικών, με αποτέλεσμα την ποικιλία της ροής δεδομένων, της καθυστέρησης και της διακοπής της σύνδεσης σε όλο το δίκτυο. Η συμμετοχή στο δίκτυο είναι υψηλά δυναμική και απρόβλεπτη, καθώς οι συνδέσεις περνούν από κατάσταση "ενεργοποίησης" και "απενεργοποίησης", και συσκευές προστίθενται και αφαιρούνται από το δίκτυο.

Η υλοποίηση του συστήματος εφαρμογής των πόρων της επιχείρησης (ERP) αποτελεί τη βάση για τη δημιουργία του έξυπνου συστήματος είτε σε επίπεδο πόλης είτε σε επίπεδο υποδομής. Η ιδέα πίσω από την υλοποίηση του ERP είναι η αντικατάσταση των υπαρχόντων συστημάτων

παλαιάς τεχνολογίας και των διαθέσιμων διεπαφών, σε ένα ενιαίο πλούσιο σε λειτουργίες προϊόν εφαρμογής (SAP). Ο σκοπός του SAP είναι να τυποποιήσει όλα τα δυνατά επιχειρηματικά μοντέλα και όλες τις λειτουργικές διαδικασίες σε μία πλατφόρμα, SMART GIS/IT (2007). Οι κατασκευαστικές δραστηριότητες για εγκαταστάσεις όπως ηλεκτρισμός, νερό, αέριο, κλιματισμός περιοχής, άρδευση, αποχέτευση και δίκτυα επικοινωνιών πρέπει να παρακολουθούνται πλήρως καθημερινά, προκειμένου να εκμεταλλευτούν τους τεράστιους πόρους και το ανθρώπινο εργατικό δυναμικό. Αυτοί οι πόροι εκχωρούνται μόνο για να καταγραφεί η λειτουργική κατάσταση για τις ενότητες κατασκευής και εκτέλεσης που θα πραγματοποιήσουν την απαιτούμενη συντήρηση. Η ανάγκη για ένα σύστημα που θα εξυπηρετεί όλα τα διευθυντικά στελέχη στην παρακολούθηση όλων αυτών των δραστηριοτήτων με κατάλληλη γεωγραφική εκπροσώπηση θα μειώσει σίγουρα το ανθρώπινο δυναμικό μακροπρόθεσμα.

Αρκετές κυβερνήσεις και μερικοί από τους κύριους κατασκευαστές ακινήτων αρχίζουν να εφαρμόζουν ένα επιχειρησιακό έργο GIS για τα παγκόσμια έργα τους, προκειμένου να διευκολύνουν τις διαδικασίες διαχείρισης έργων στο πλαίσιο της έννοιας της ψηφιακής υποδομής. Η Ομάδα Εργασίας του Έξυπνου Συμβουλίου Κράτους (2006) ανέπτυξε την υλοποίηση του έξυπνου συνεπιχειρησιακού σχεδίου στην κυβέρνηση του Κουίνσλαντ. Αυτό έγινε προκειμένου να παρέχει συμβουλευτικές υπηρεσίες υψηλού επιπέδου για τα αναδυόμενα θέματα και τις τάσεις του έξυπνου κράτους. Το δυναμικό στις κύριες εταιρείες ανάπτυξης ακινήτων είναι η κλίμακα των έργων και η τεράστια ανθρώπινη δύναμη που χρησιμοποιούν στα έργα ανάπτυξης ακινήτων. Κατά συνέπεια, κατασκευάζουν αρκετές πόλεις σε ολόκληρο τον κόσμο. Λόγω αυτού του ευρέος φάσματος δραστηριοτήτων ανάπτυξης ακινήτων, πρέπει να γίνει λεπτομερής μελέτη των υφιστάμενων συστημάτων με όλες τις σχετικές μηχανές βάσεων δεδομένων και επιχειρηματικές πλατφόρμες. Η μελέτη αποσκοπεί στη δημιουργία του μοντέλου λειτουργίας των πλαισίων δικτύων υποδομής/υπηρεσιών κοινής ωφέλειας.



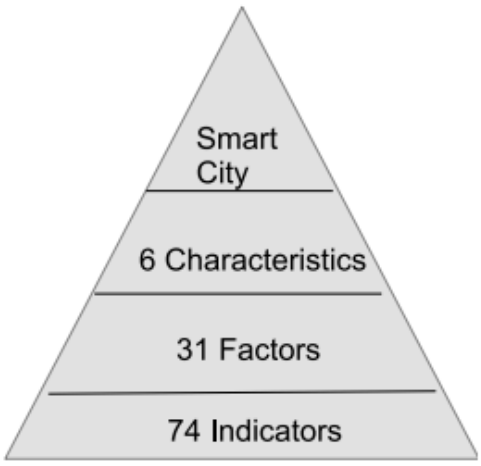
Εικόνα 4 Πλαίσιο ανάπτυξης και παρακολούθησης υποδομών έξυπνης πόλης

3.4 : Μοντέλα έξυπνων πόλεων

Για να γίνει η έξυπνη πόλη πραγματικότητα, κορυφαίες επιχειρηματικές εταιρείες, επαγγελματίες της έξυπνης πόλης και ακαδημαϊκοί ερευνητές εργάζονται τα τελευταία χρόνια για την ανάπτυξη πλαισίων. Για την ώρα, οι πιο ανεπτυγμένες πόλεις σε όλο τον κόσμο είχαν σημειώσει σημαντική πρόοδο. Ωστόσο, οι μικρές και αναδυόμενες πόλεις εξακολουθούν να αντιμετωπίζουν προκλήσεις στην εφαρμογή αυτής της νέας έννοιας.

Η διαδικασία διάρθρωσης του μοντέλου έξυπνης πόλης πρέπει να βασίζεται σε μια ολοκληρωμένη και συγκριτική μελέτη των σημερινών ιστοριών επιτυχίας. Η έξυπνη πόλη χρησιμοποιείται για την καθιέρωση της έξυπνης λειτουργίας σε βιομηχανικούς, εκπαιδευτικούς και κυβερνητικούς τομείς, χωρίς να ξεχνάμε τη χρήση των σύγχρονων τεχνολογιών στην καθημερινή ζωή, πράγμα που σημαίνει ότι υπάρχουν

σημαντικά πεδία δραστηριοτήτων στον όρο έξυπνη πόλη, κάτι που οδήγησε τον R. Giffinger να προσδιορίσει 6 χαρακτηριστικά, τα οποία είναι: "Έξυπνη οικονομία, έξυπνο περιβάλλον, έξυπνη διακυβέρνηση, έξυπνη διαβίωση, έξυπνη κινητικότητα και έξυπνοι άνθρωποι".
Η πρώτη δομή του μοντέλου παρουσιάζεται ως ιεραρχικό τρίγωνο (Figure 5) προκειμένου να εκφράσει τις πτυχές της Έξυπνης Πόλης. Επιπλέον, κάθε χαρακτηριστικό ορίζεται από ορισμένους παράγοντες.



Εικόνα 5 Δομή μοντέλου

Εκ πρώτης όψεως, το όραμα μιας πόλης πρέπει να είναι με τη συμμετοχή των κατοίκων. Έτσι, οι πόλεις θα πρέπει πρώτα να θέσουν ένα σημείο εκκίνησης πριν από τη δημιουργία , κοιτάζοντας προς τα εμπρός. Στη συνέχεια, θα είναι δυνατή η τοποθέτηση δεικτών. Μια πόλη , χρειάζεται ένα σημείο αναφοράς το οποίο είναι πρωταρχικό για τον καθορισμό κάθε πόλης, δεδομένου ότι οι ανάγκες είναι διαφορετικές από πόλη σε πόλη, όπως οι ανάγκες και οι προκλήσεις, οι οποίες λαμβάνουν υπόψη την πυκνότητα του πληθυσμού, τοπογραφία και τις υποδομές ως βασικά στοιχεία. Οι πόλεις θα πρέπει να ακολουθούν τις αρχές της “Λιτής Εκκίνησης” (lean start up). Στον ίδιο πλαίσιο, η Διεθνής Επιχείρηση Μηχανών (IBM) υπογραμμίζει το 3D όραμά της , έναντι του έξυπνου κατάλληλου αστικού χώρου. Οι τρεις πυλώνες είναι: Οι Άνθρωποι, η υποδομή και οι λειτουργίες. Σύμφωνα με αυτό, έχουν καθοριστεί τρεις υπηρεσίες, οι οποίες είναι: Ανθρώπινες υπηρεσίες που περιλαμβάνουν εκπαίδευση, υγειονομική περίθαλψη και κοινωνικά προγράμματα των

κατοίκων, υπηρεσίες υποδομής που αποτελούνται από ενέργεια, νερό , μεταφορές , σχεδιασμό και διαχείριση που ομαδοποιούν όλη τη διακυβέρνηση της πόλης, τη δημόσια ασφάλεια, τον αστικό σχεδιασμό και τη διαχείριση των φυσικών πόρων. Ακόμα κι αν η λίστα μοντέλων υπογραμμίζει την ετερογένεια του έξυπνου αστικού concept, η πλειονότητα των μοντέλων έχουν κάποια κοινά χαρακτηριστικά. Μπορούμε να συμπεράνουμε ότι υπάρχουν 6 διαστάσεις που αποτελούν μέρος των περισσότερων μοντέλων: Έξυπνη Υγεία-Ζωή, Έξυπνη Διακυβέρνηση, Έξυπνη Οικονομία, Έξυπνη Κινητικότητα, Έξυπνο Περιβάλλον και Έξυπνη Διαβίωση.

3.5: Τα πλεονεκτήματα των smart city

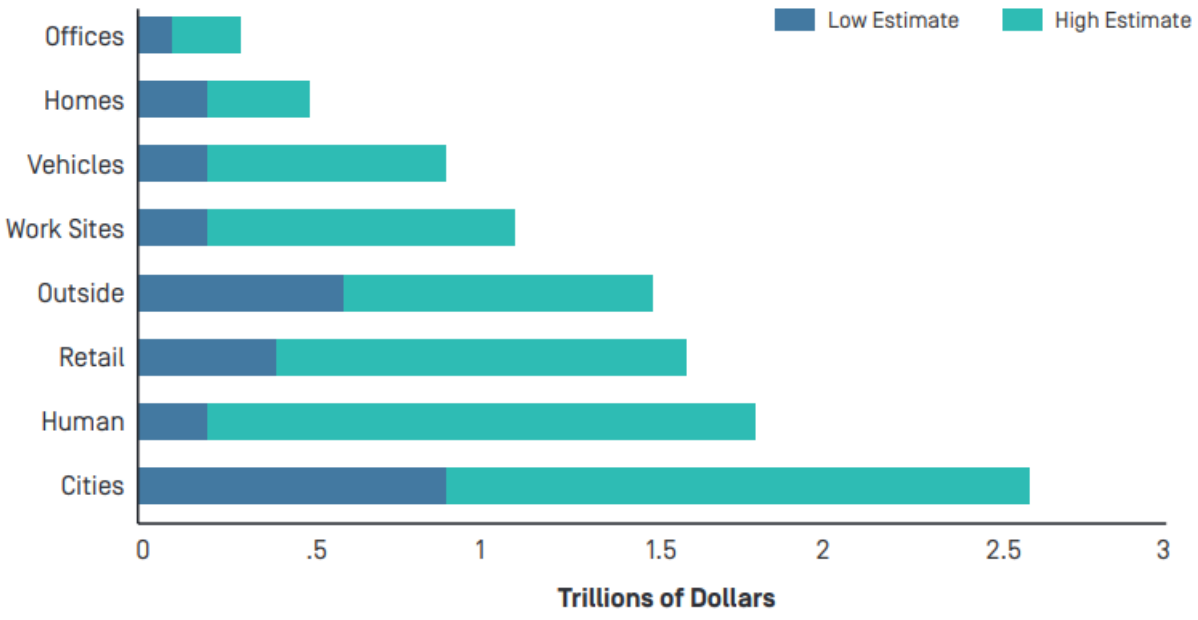
Το "Διαδίκτυο των Πραγμάτων" περιγράφει τη δυνατότητα σύνδεσης οποιασδήποτε συσκευής - που υποστηρίζει το πρωτόκολλο Internet Protocol -με το Διαδίκτυο. Σύμφωνα με μία αναφορά Big Data, "Αυτές οι συσκευές μπορεί να περιλαμβάνουν το θερμοστάτη σας, το αυτοκίνητό σας ή ένα χάπι που καταπίνετε ώστε ο γιατρός να μπορεί να παρακολουθεί την υγεία του πεπτικού σας συστήματος." Ο αριθμός των νέων συσκευών και υπηρεσιών που χτίζονται για το IoT έχει αυξηθεί σημαντικά τα τελευταία χρόνια, και προβλέπεται ότι μεταξύ του 2020 θα χρησιμοποιούνται παγκοσμίως από 26 έως 50 δισεκατομμύρια συνδεδεμένες συσκευές. Με τον αριθμό των συσκευών να αυξάνεται εκθετικά κάθε χρόνο, το IoT μπορεί να προσφέρει ένα πιθανό παγκόσμιο οικονομικό αντίκτυπο από 4 τρισεκατομμύρια έως 11 τρισεκατομμύρια δολάρια ετησίως μέχρι το 2025. Η μεγαλύτερη επίδραση αναμένεται να γίνει αισθητή σε αστικές περιοχές όπου οι συσκευές IoT και οι "έξυπνες" τεχνολογίες έχουν τη δυνατότητα να εκμεταλλευτούν δίκτυα επικοινωνίας υψηλής ταχύτητας για την ενίσχυση της υποδομής και των υπηρεσιών όπως η παροχή νερού και ηλεκτρικού ρεύματος, η υγιεινή και η διαχείριση απορριμμάτων, η αστική κινητικότητα και η δημόσια συγκοινωνία, η συνδεσιμότητα Πληροφορικής, η δημόσια ασφάλεια και η παρακολούθηση του καιρού. Το 2014, λίγο μετά την ορκωμοσία της

κυβέρνησής του, ο Ινδός πρωθυπουργός Ναρέντρα Μόντι ανακοίνωσε το όραμά του για τη δημιουργία 100 έξυπνων πόλεων σε ολόκληρη τη χώρα. Ορίζει μια έξυπνη πόλη ως μια πόλη εξοπλισμένη με βασική υποδομή για να προσφέρει ποιότητα ζωής και ένα καθαρό και βιώσιμο περιβάλλον μέσω της εφαρμογής έξυπνων λύσεων. Η έννοια των έξυπνων λύσεων του Μόντι περιστρέφεται γύρω από τρεις περιοχές:

1) Ηλεκτρονική διάδοση πληροφοριών μεταξύ τοπικών αρχών και πολιτών για την αυτόματη γνωστοποίηση ειδοποιήσεων και τη δυνατότητα γρήγορης ανατροφοδότησης των πολιτών.

2) Βελτιωμένη διαχείριση ενέργειας μέσω της χρήσης αυτοματοποιημένων μετρητικών ελέγχων και ανάπτυξης ‘’πράσινων’’ κτιρίων.

3) Προηγμένη ανάλυση και έξυπνα συστήματα διαχείρισης κίνησης για την υποστήριξη της αποτελεσματικής χρήσης του αστικού οδικού δικτύου.



Εικόνα 6 Πιθανή Παγκόσμια Οικονομική Επίδραση, ανάλογα με τις ρυθμίσεις που χρησιμοποιεί το Διαδίκτυο των Πραγμάτων

Το σχέδιο του Modi για έξυπνες πόλεις και η χρήση της Πληροφορικής και Επικοινωνιών για τη δημιουργία έξυπνων λύσεων δεν περιορίζεται στην Ινδία. Πολλές έξυπνες πόλεις χρησιμοποιούν την Πληροφορική και τις επικοινωνίες για τη δημιουργία νέων τρόπων διαχείρισης των συστημάτων μεταφοράς της πόλης, της διανομής ψηφιακής ενέργειας, του ελέγχου της κυκλοφορίας και της παρακολούθησης της περιβαλλοντικής ρύπανσης. Μέσα στις έξυπνες πόλεις, η τεχνολογία αυτοματισμού κτιρίων προσφέρει σημαντικές προόδους στη φυσική ασφάλεια, την ψύξη και θέρμανση του χώρου και τον έλεγχο του φωτισμού. Οι εξελίξεις στην τεχνολογία κατασκευής συμβάλλουν στη συνεχή παρακολούθηση κατάστασης, στα «έξυπνα» εργοστάσια και στην ασύρματη κινητή παρακολούθηση της αλυσίδας εφοδιασμού. Τα έξυπνα πλέγματα και η υποδομή για ηλεκτρικά οχήματα προσφέρουν μεγάλες προοπτικές για βελτίωση της αποδοτικότητας σε περιβάλλοντα με περιορισμένη ενέργεια. Συνολικά, το Διαδίκτυο των Πραγμάτων δίνει τη δυνατότητα για πιο αποδοτική χρήση των πόρων, βελτιώσεις στις υπηρεσίες και την ασφάλεια και δημιουργεί μεγαλύτερο αίσθημα σύνδεσης μέσα στις αναδυόμενες έξυπνες πόλεις.

Τα οφέλη που συνδέονται με τις Έξυπνες Πόλεις είναι οικονομικά, κοινωνικά και πολιτικά, αλλά πολλοί από τους υπεύθυνους αυτών των πρωτοβουλιών είναι τεχνολογικής φύσης. Σύμφωνα με την Goldman Sachs, υπάρχουν πέντε βασικές τεχνολογίες που οδηγούν την εξάπλωση του Διαδικτύου των Πραγμάτων, οι οποίες, αντίστοιχα, υποστηρίζουν τις προσπάθειες για Έξυπνες Πόλεις:

- **Φθηνό εύρος ζώνης**: Το κόστος της ζώνης έχει πέσει κατακόρυφα, κατά περίπου 40 φορές τα τελευταία 10 χρόνια.

- **Φθηνή επεξεργασία**: Ο "νόμος του Moore" μας λέει ότι στην ιστορία του υπολογιστικού υλικού, ο αριθμός των τρανζίστορ σε ενσωματωμένα κυκλώματα διπλασιάζεται περίπου κάθε δύο χρόνια. Με παρόμοιο τρόπο, τα κόστη επεξεργασίας έχουν μειωθεί κατά περίπου 60 φορές τα τελευταία 10 χρόνια, επιτρέποντας σε περισσότερες συσκευές να μην είναι απλώς

συνδεδεμένες, αλλά αρκετά έξυπνες για να ξέρουν τι να κάνουν με όλα τα νέα δεδομένα που παράγονται ή λαμβάνονται.

- **Έξυπνα κινητά τηλέφωνα**: Τα έξυπνα κινητά τηλέφωνα γίνονται πλέον η προσωπική πύλη πρόσβασης στο Διαδίκτυο των Πραγμάτων (IoT), λειτουργώντας ως τηλεχειριστήριο ή κέντρο ελέγχου για το συνδεδεμένο σπίτι, το συνδεδεμένο αυτοκίνητο ή τις συσκευές υγείας και φυσικής κατάστασης που οι καταναλωτές αρχίζουν όλο και περισσότερο να φορούν.

- **Πανταχού ασύρματη κάλυψη με Wi-Fi:** Η κάλυψη του Wi-Fi μεταφέρεται τώρα σε γρήγορη υιοθέτηση του 4G LTE, σχεδόν παντού η ασύρματη συνδεσιμότητα είναι διαθέσιμη δωρεάν ή σε πολύ χαμηλό κόστος, καθώς το WiFi χρησιμοποιεί μη αδειοδοτημένο φάσμα και, συνεπώς, δεν απαιτεί μηνιαία τέλη πρόσβασης σε φορέα.

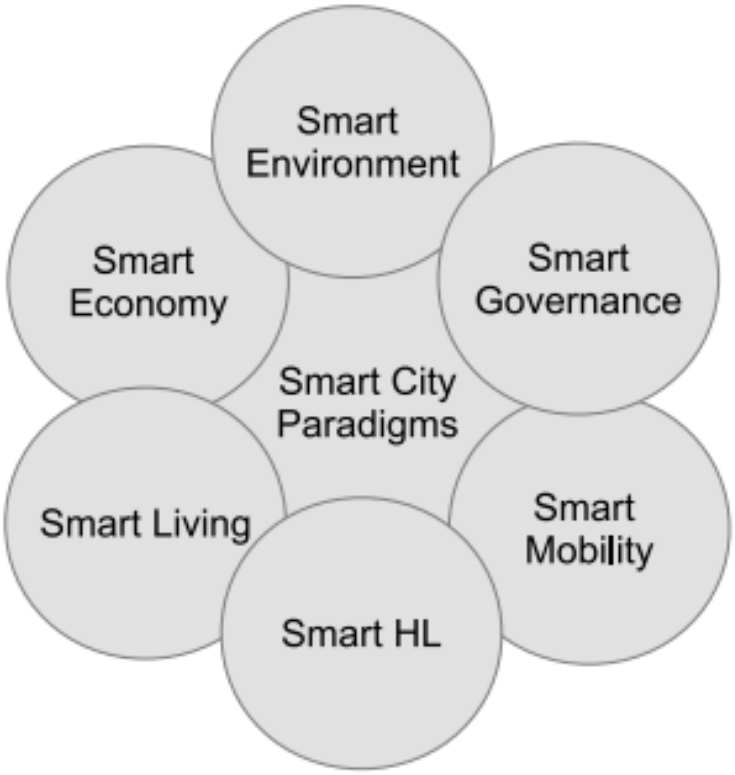
- **Μεγάλα δεδομένα**: Δεδομένου ότι το IoT θα παράγει αναπόφευκτα όγκους δεδομένων, η διαθεσιμότητα του νέφους / λογισμικού ως υπηρεσία και η ανάλυση μεγάλων δεδομένων αποτελεί κλειδί για την εξέλιξη.

Συνοπτικά, το κόστος σύνδεσης έχει μειωθεί ενώ έχουν αναπτυχθεί νέοι τρόποι ανάλυσης μεγάλων ποσοτήτων δεδομένων. Ως αποτέλεσμα, τόσο οι κυβερνήσεις όσο και οι εταιρείες επικεντρώνονται στο Διαδίκτυο των Πραγμάτων ως κινητήριο δύναμη για την τεχνολογική καινοτομία και τις νέες δυνατότητες. Για παράδειγμα, το 2014 η AT&T εισήγαγε την υπηρεσία «Connected Car» στις Ηνωμένες Πολιτείες σε συνεργασία με αρκετούς κατασκευαστές αυτοκινήτων, συμπεριλαμβανομένων των Audi, GM, Tesla και Volvo. Αυτή η υπηρεσία πρόσφερε υψηλής ταχύτητας συνδέσεις 3G ή 4G με μηνιαία συνδρομή $10, επιτρέποντας έτσι στα οχήματα να λειτουργούν ως Wi-Fi hotspots με σύνδεση για έως και επτά συσκευές, καθώς επίσης να έχουν πρόσβαση στο σύστημα «OnStar» για ανάγκες έκτακτης βοήθειας και απομακρυσμένης διάγνωσης οχήματος. Έως το 2015, τριάντα μοντέλα της GM προσέφεραν αυτήν την υπηρεσία. Για να βελτιωθεί η παραγωγικότητα και να εξοικονομηθούν κόστη, οι επιχειρήσεις υιοθετούν επίσης το Διαδίκτυο των

Πραγμάτων, ιδιαίτερα στους τομείς της εργασίας και της ενέργειας. Για παράδειγμα, στην Σιγκαπούρη, η χρήση ενός λογισμικού ορισμού λογισμικού μεταβλητών δεδομένων οδηγεί σε εξοικονόμηση λειτουργικών δαπανών έως και 30% ανά επιχείρηση. Ένα κρίσιμο κομμάτι της ιστορίας είναι η επέκταση της υποδομής που υποστηρίζει τις επικοινωνίες βασισμένες στο Διαδίκτυο, συμπεριλαμβανομένων των οπτικών ινών, των δορυφορικών δικτύων και των ασύρματων δικτύων. Ταυτόχρονα, η γρήγορη διάδοση των προσωπικών ηλεκτρονικών συσκευών, των αισθητήρων και των υποδομών υπολογιστικού νέφους έχει δημιουργήσει ένα δίκτυο δισεκατομμυρίων κομματιών λογισμικού και υλικού που μπορούν τώρα να δημιουργούν, επεξεργάζονται και ανταλλάσσουν δεδομένα. Το 90% των δεδομένων του κόσμου σήμερα δημιουργήθηκε τα τελευταία δύο χρόνια και αναμένεται ότι αυτά τα δεδομένα θα διπλασιάζονται κάθε δύο χρόνια μέχρι το έτος 2020. Σε συνδυασμό με την παγκόσμια συνδεσιμότητα και τα μεγάλα δεδομένα, το Διαδίκτυο των Πραγμάτων δημιουργεί ανησυχίες σχετικά με την απειλή της ευπάθειας, την συνολική ασφάλεια και την ιδιωτικότητα. Τις ανησυχίες αυτές θα τις αναλύσουμε παρακάτω λεπτομερώς.

3.6: Οι εφαρμογές των smart cities:

Μπορούμε να αναζητήσουμε πολλά στοιχεία επίγνωσης, ευελιξίας, μετασχηματισμού, συνεργατικότητας, ατομικότητας, αυτοδιάθεσης και στρατηγικής προσέγγισης για την επίτευξη της ευφυΐας. Καθώς η πόλη είναι ένα σύνολο συστημάτων, αρκετές έρευνες εντόπισαν ορισμένα χαρακτηριστικά που εξασφαλίζουν την πραγματική ευφυΐα της πόλης και, ως εκ τούτου, καθιστούν τον Όρο της Έξυπνης Πόλης πιο συγκεκριμένο. Το ευρωπαϊκό έργο βασίστηκε σε ιεραρχική δομή με σκοπό να παρουσιάσει τη σχέση μεταξύ επιπέδων ανάλυσης. Επομένως, κάθε χαρακτηριστικό ορίζεται από ορισμένους παράγοντες, όπως φαίνεται στην εικόνα 7.



Εικόνα 7 Χαρακτηριστικά Έξυπνων Πόλεων

Η Έξυπνη Οικονομία περιγράφεται από την καινοτόμο, επιχειρηματική, παραγωγική, ευέλικτη οικονομία, τα εμπορικά σήματα και την ένταξη σε όλους τους τύπους αγορών. Για τους Έξυπνους Ανθρώπους, βλέπουμε την ανάπτυξη του Ανθρώπινου Κεφαλαίου όσον αφορά την εκπαίδευσή τους και την ποιότητα της κοινωνικής τους αλληλεπίδρασης. Η Έξυπνη Διακυβέρνηση περιλαμβάνει όλες τις πολιτικές, διοικητικές και δημόσιες υπηρεσίες. Μπορούμε επίσης να περιγράψουμε την Έξυπνη Κινητικότητα μέσω της ευρείας προσβασιμότητας, της διαθεσιμότητας των ΤΠΕ και της βιωσιμότητας νέων συστημάτων. Το Έξυπνο Περιβάλλον που μπορεί να επιτευχθεί χάρη στην επίδραση σε ελκυστικές φυσικές συνθήκες και σχέδια προστασίας του περιβάλλοντος, καθώς και την Έξυπνη Ζωή που περιλαμβάνει όλες τις πτυχές της ποιότητας ζωής.

3.6.1: Έξυπνη οικονομία (Smart Economy)

Σημαντικές έρευνες έχουν αποκαλύψει την απουσία του καθολικού ορισμού της Έξυπνης Οικονομίας και έχουν περιγράψει τον όρο με διαφορετικούς τρόπους. Περιλαμβάνει έξυπνες εταιρείες που παράγουν καινοτόμες ιδέες και βελτιώνουν την αναλογία τιμής-ποιότητας βασιζόμενες στον συνειδητό πόρο. Ωστόσο, αυτός ο ορισμός δεν έδειξε όλες τις συγκεκριμένες πλευρές της Έξυπνης Οικονομίας. Γι' αυτό το λόγο, οι ερευνητές συνεχίζουν να αναπτύσσουν περισσότερους ορισμούς. Σύμφωνα με τους ερευνητές, εδώ είναι κάποια κοινά χαρακτηριστικά της Έξυπνης Οικονομίας:

Καινοτόμο ιδέες: που αυξάνουν την παραγωγικότητα και μειώνουν το κόστος. Ψηφιακή· εκτεταμένη χρήση των ΤΠΕ στην οικονομία.
Ανταγωνιστική: να είναι ανοιχτή, να αξιοποιεί τη γνώση και την καινοτομία για να αποκτήσει καλή ποιότητα υψηλότερα κέρδη, παραγωγικούς πόρους και αποτελεσματικά κόστη.
Πράσινη: εστίαση στις βιώσιμες αρχές, χρήση φυσικών πηγών ενέργειας και ανάκτηση καθαρών περιοχών.
Κοινωνικά υπεύθυνη: επιδίωξη προώθησης της ευημερίας των ατόμων.

3.6.2: Έξυπνο περιβάλλον (Smart Environment)

Για να αυξήσει τη βιωσιμότητα, η πόλη πρέπει να ενεργήσει σε περιβαλλοντικές υποδομές οι οποίες είναι: υδάτινες οδοί, αγωγοί αποχέτευσης και πράσινοι χώροι. Θα πρέπει επίσης να βασίζεται στη χρήση φυσικών και πράσινων πηγών ενέργειας.

3.6.3: Έξυπνη κυβέρνηση (Smart Governance)

Το σύνολο των έξυπνων έργων πόλης περιλαμβάνει τη συμμετοχή πολλών εμπλεκόμενων φορέων. Για να διαχειριστούν καλύτερα

αυτά τα έργα και να παίρνονται πρωτοβουλίες, οι πόλεις πρέπει να βελτιώσουν την ποιότητα της διακυβέρνησης. Γενικά, η παραδοσιακή διακυβέρνηση είναι "ως καθεστώτα νόμων, διοικητικών κανόνων, δικαστικών αποφάσεων και πρακτικών που περιορίζουν, καθορίζουν και δυναμώνουν τη δραστηριότητα της κυβέρνησης, όπου αυτή η δραστηριότητα ορίζεται ευρέως ως η παραγωγή και παράδοση δημοσίως υποστηριζόμενων αγαθών και υπηρεσιών". Χάρη στην εμφάνιση των ΤΠΕ, οι πόλεις προσπαθούν να προωθήσουν την κυβέρνησή τους, έτσι, όλες οι δραστηριότητες διακυβέρνησης που βασίζονται στην τεχνολογία είναι έξυπνες διακυβερνήσεις. Αντιπροσωπεύει "ένα σύνολο τεχνολογιών, ανθρώπων, πολιτικών, πρακτικών, πόρων, κοινωνικών κανόνων και πληροφοριών που αλληλοεπιδρούν για να υποστηρίξουν τις δραστηριότητες διακυβέρνησης της πόλης". Βελτιώνει τα συστήματα πληροφοριών και τις επικοινωνιακές δικτυώσεις και χρησιμοποιεί καινοτόμες πολιτικές, τεχνολογία και μοντέλα επιχειρήσεων. Σε μελέτη που πραγματοποιήθηκε, η επιτυχία των έργων ηλεκτρονικής διακυβέρνησης εξαρτάται από τις σχέσεις μεταξύ των φορέων ενδιαφέροντος όπου "οι σχέσεις μεταξύ των φορέων ενδιαφέροντος αναφέρονται σε τέσσερα κύρια θέματα: η δυνατότητα συνεργασίας μεταξύ των φορέων ενδιαφέροντος, η υποστήριξη της ηγεσίας, η δομή των συμμαχιών και η εργασία υπό διαφορετικές δικαιοδοσίες".

3.6.4: Έξυπνη ζωή (Smart Living)

Στον συνδυασμό όλων των αξόνων που έχουν παρουσιαστεί, οι πολίτες αναπτύσσουν έξυπνους τρόπους ζωής μέσω της τεχνολογίας. Όλα συνδέονται σε συσκευές δικτύωσης, οπότε πολλές εργασίες γίνονται πιο εύκολες, ασφαλείς και φθηνότερες. Τα τελευταία χρόνια, οι καινοτόμες λύσεις υπό ανάπτυξη τείνουν να κάνουν τη ζωή των ατόμων πιο παραγωγική, βιώσιμη και αποτελεσματική. Για παράδειγμα, η λειτουργία έξυπνων κτιρίων έχει κερδίσει ενδιαφέρον και η σύνδεση συστημάτων κτιρίων,

μέρος των σύγχρονων κτιρίων εξοπλισμένων με στοιχεία και τεχνολογικές συσκευές, στοχεύει στο να δημιουργήσει μαζί ένα σύνολο ευφυούς συλλογικής νοημοσύνης και να φέρει ένα σύνολο χαρακτηριστικών για να βελτιώσει την παραγωγικότητα, την ασφάλεια και την άνεση των κατοίκων. Ένας διαχειριστής κτιρίου, ως ένα σύνολο στρωμάτων ενός πρότυπου αυτοματισμού, συγκεντρώνει δεδομένα, αναλύει, παρακολουθεί και διαχειρίζεται το κτίριο σύμφωνα με το παράδειγμα του Διαδικτύου των Πραγμάτων.

3.6.5: Έξυπνη κινητικότητα (Smart Mobility)

Η ιστορία των αστικών μεταφορών γνώρισε πολλές αλλαγές που προκλήθηκαν από διάφορες επιλογές ταξιδιών των ανθρώπων και οδήγησαν στη γέννηση τριών τύπων πόλεων. Πρώτον, οι Πόλεις Περιπάτου ήταν μια ιδέα που προτάθηκε από τον βρετανό αρχιτέκτονα Ρον Χέρον το 1964. Χαρακτήρισε αυτόν τον τύπο, αφενός, με στενούς δρόμους, οι οποίοι συνδέουν σημαντική πυκνότητα πληθυσμού με ανάμεικτη χρήση γης και, αφετέρου, με επίτευξη προορισμών σε μισή ώρα με τα πόδια. Επιπλέον, οι Πόλεις Μεταφορών ήταν ένα σχέδιο για την ανάπτυξη των δημόσιων μεταφορών στο Τορόντο του Οντάριο, Καναδά. Προτάθηκε και ανακοινώθηκε για πρώτη φορά από τον Ντέιβιντ Μίλερ το 2007 με στόχο την ενσωμάτωση των σιδηροδρομικών γραμμών τρένων και των δρομολογίων τραμ προκειμένου να καταστήσει τις πόλεις πιο λειτουργικές με μείωση της πυκνότητας πληθυσμού. Η Αυτοκινητόπολη είναι ένας τύπος πόλης στον οποίο τα μέσα μεταφοράς είδαν σημαντική αλλαγή μετά τον Δεύτερο Παγκόσμιο Πόλεμο. Η ύπαρξη αυτού του είδους οφείλεται στην τεχνολογική ανάπτυξη των μέσων μεταφοράς με σκοπό την ταχεία μετακίνηση προς οποιαδήποτε κατεύθυνση και προς οποιοδήποτε προορισμό, με την διαίρεση της πόλης σε διαφορετικά λειτουργικά μέρη, μειώνοντας την πυκνότητα πληθυσμού κοντά στις μεταφορικές δυνατότητες.

Η εξέλιξη των μητροπολιτικών περιοχών σε όλο τον κόσμο οδηγεί σε μετασχηματισμό των τρόπων ζωής και πρακτικών κινητικότητας: οι άνθρωποι μετακινούνται χρησιμοποιώντας ποικίλα μέσα μεταφοράς, όλο και περισσότερο για λόγους που γίνονται όλο και πιο ποικίλοι. Για να ληφθεί υπόψη τόσο η πολυπλοκότητα των πρακτικών κινητικότητας όσο και η ισχυρή σύνδεση μεταξύ των αστικών μετασχηματισμών και των κινήσεων, επιστήμονες και τεχνικοί χρησιμοποιούν έναν νέο όρο: "Αστική Κινητικότητα". Προβλήματα κυκλοφορίας όπως οι συμφορήσεις, οι μακρές ουρές και οι καθυστερήσεις, δεν είναι καινούργια φαινόμενα για τις αστικές περιοχές και δεν είναι αποκλειστικά για μεγαλουπόλεις. Ο Έλεγχος Τροχαίας στις Αστικές Περιοχές (Urban Traffic Control - UTC) και τα Συστήματα Διαχείρισης Κυκλοφορίας (Traffic Management Systems - TMS) έχουν γνωρίσει τεράστια εξέλιξη μέσα στα χρόνια, από τότε που εφαρμόστηκαν οι πρώτοι φωτεινοί σηματοδότες στο δεύτερο μισό του 19ου αιώνα. Με την αύξηση της ανθρώπινης πληθυσμιακής αύξησης και των αυτοκινήτων, τα συστήματα ελέγχου κυκλοφορίας στην αστική υποδομή πρέπει να σχεδιάζουν στρατηγικές για να ανταποκριθούν στις μελλοντικές απαιτήσεις κινητικότητας. Ενώ διατηρούν τον αρχικό σκοπό τους να βελτιστοποιούν την εξυπηρέτηση και να εγγυώνται την ποιότητα των υπηρεσιών, βασικά συστατικά της αστικής έξυπνης ανάπτυξης, όπως οι Τεχνολογίες Πληροφορικής και Επικοινωνιών και το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT), εξετάζονται πλέον για να αξιοποιήσουν τα συστήματα ελέγχου κυκλοφορίας νέας γενιάς.

3.7: Έξυπνες πόλεις στην Ελλάδα

3.7.1: Η έξυπνη πόλη των Τρικάλων

Τα Τρίκαλα έχουν τη διάκριση της πρώτης «Έξυπνης Πόλης» στην Ελλάδα ενσωματώνοντας τεχνολογικά προηγμένες λύσεις στην καθημερινή ζωή της Δημοτικής Αρχής, προσφέροντας στους πολίτες κυβερνητικές υπηρεσίες μέσω μιας πλατφόρμας ηλεκτρονικής διακυβέρνησης. Ξεκινώντας από την ελεύθερη πρόσβαση στο Ίντερνετ μέσω Wi-Fi σε ολόκληρο τον αστικό ιστό, σε τηλεϊατρικές υπηρεσίες για τους πολίτες τρίτης ηλικίας, λεωφορεία χωρίς οδηγό, στην διαδικτυακή πλατφόρμα e-Dialogos μέσω της οποίας οι δημότες έχουν τη δυνατότητα να συμμετέχουν στη δημόσια ζωή της πόλης και τη διαδικασία λήψης αποφάσεων, τα Τρίκαλα χρησιμοποιούν την τεχνολογία για την αύξηση της διαφάνειας και τη βελτίωση της ζωής των δημοτών.

Εντύπωση προκαλεί ο τρόπος με τον οποίον η δημοτική αρχή και ο Γενικός Διευθυντής της πλατφόρμας e-Trikala ενσωμάτωσαν την τεχνολογία ως μέσο προκειμένου να φέρουν την κυβέρνηση πιο κοντά στους πολίτες και οργάνωσης της παροχής δημοτικών υπηρεσιών. Τα Τρίκαλα αποτελούν ηγετικό μοντέλο του 21ου αιώνα και για άλλες Ελληνικές πόλεις που προσπαθούν να δημιουργήσουν συνεργασίες με αμερικανικές επιχειρήσεις προκειμένου να θέσουν την τεχνολογία στην υπηρεσία της δημοκρατίας. Με την τεχνολογία να παίζει τέτοιο σημαντικό ρόλο στην πόλη, τα Τρίκαλα αποτελούν έναν εξαιρετικό οικοδεσπότη για πρόγραμμα CodeGirls 2.0.

Το πρόγραμμα CodeGirls υποστηρίζεται από την Αμερικανική Πρεσβεία στην Αθήνα και τον εταίρο μας, την Ελληνική Μη Κυβερνητική Οργάνωση ΜΑΤΑΡΟΑ, και στόχο έχει να διδάξει σε νεαρά κορίτσια τις βασικές αρχές δημιουργίας ιστοσελίδων. Μια νέα γυναίκα ήδη φοιτά στο Αμερικανικό Κολλέγιο και κατόπιν διαγωνισμού της προσφέρθηκε θέση πρακτικής από τεχνολογική εταιρία μετά την παρακολούθηση του προγράμματος CodeGirls της Καλαμάτας.

Το φιλικό προς την τεχνολογία πνεύμα των Τρικάλων επίσης εμπνέει και υποστηρίζει την επιχειρηματικότητα. Στα Τρίκαλα συναντάμε επίσης το EasyBike. Το EasyBike είναι το πρώτο σύστημα κοινής χρήσης

ποδηλάτων που θα αναπτυχθεί και εφαρμοσθεί με επιτυχία στην Ελλάδα. Το σύστημα αυτό ήδη λειτουργεί 30 εν ενεργεία προγράμματα κοινής χρήσης ποδηλάτων σε διάφορες πόλεις με περισσότερα από 2.500 ποδήλατα, της Αθήνας περιλαμβανομένης. Η πρωτοβουλία αυτή προωθεί τη βιώσιμη κινητικότητα και αποτελεί παράδειγμα για το πώς επιχειρηματίες στον χώρο της τεχνολογίας μπορούν να επιτύχουν στην Ελλάδα σε συνεργασία με Οργανισμούς Τοπικής Αυτοδιοίκησης.
Επιχειρηματίες και νεοφυείς επιχειρήσεις μπορούν πραγματικά να επιτύχουν όταν έχουν τέτοια κυβερνητική συμπαράσταση σε τοπικό και εθνικό επίπεδο.

3.7.2: Η έξυπνη πόλη της Χαλκίδας

Το δρόμο προς την «έξυπνη πόλη» δείχνει πλέον η Χαλκίδα, όπου εγκαταστάθηκαν και λειτουργούν πιλοτικά «έξυπνα» συστήματα στάθμευσης (Smart Parking), φωτισμού (Smart Lighting) και μέτρησης περιβαλλοντικών παραμέτρων (Air Quality Monitoring), καθώς και μια ενιαία πλατφόρμα διαχείρισής τους. Το έργο, που υλοποίησαν από κοινού ο Όμιλος ΟΤΕ, η Cisco, η ΚΑΥΚΑΣ και η OTS, αποδεικνύει στην πράξη πώς η υιοθέτηση «έξυπνων» τεχνολογιών συμβάλλει στη βελτίωση της ποιότητας ζωής και της καθημερινότητας των κατοίκων μιας πόλης.
Με την εφαρμογή «έξυπνων» λύσεων στη Χαλκίδα, ο Όμιλος ΟΤΕ, η Cisco, η OTS και ο ΚΑΥΚΑΣ, δείχνουμε στην πράξη πώς μπορούμε να κάνουμε τις πόλεις μας πιο λειτουργικές, να προστατεύσουμε το περιβάλλον, να μειώσουμε λειτουργικά κόστη και να προσφέρουμε καλύτερη ποιότητα ζωής.
«Έξυπνες» λύσεις για στάθμευση και φωτισμό με ενιαία πλατφόρμα διαχείρισης».
Η λύση «έξυπνης» στάθμευσης, σε συνδυασμό με το mobile application που αναπτύχθηκε από την OTS και είναι διαθέσιμο για συσκευές Android και iOS, δίνει τη δυνατότητα στους οδηγούς να ενημερώνονται για τα σημεία όπου υπάρχουν ελεύθερες θέσεις στάθμευσης και πώς θα φτάσουν σε αυτές, αλλά και να καθοδηγηθούν σε άλλη θέση σε

περίπτωση που η αρχική καταληφθεί. Η εφαρμογή αναμένεται να συμβάλει σημαντικά στη μείωση του χρόνου εύρεσης θέσης στάθμευσης και κατ' επέκταση στην αποσυμφόρηση της κυκλοφορίας και την εκπομπή ρύπων. Παράλληλα, επιτρέπει στη Δημοτική Αρχή να διαχειρίζεται αποτελεσματικότερα τις θέσεις στάθμευσης, έχοντας εικόνα τόσο για το χρόνο στάθμευσης κάθε οχήματος, όσο και για κάθε στάθμευση που παραβιάζει τον Κ.Ο.Κ.

Τα συστήματα «έξυπνου» φωτισμού τεχνολογίας SSL/LED της ΚΑΥΚΑΣ, αντικατέστησαν τα φωτιστικά συστήματα συμβατικής τεχνολογίας και έχουν ήδη συμβάλλει σε εξοικονόμηση ενέργειας πάνω από 60%.Μέσω της ασύρματης διαχείρισής τους, παρέχουν τη δυνατότητα παρακολούθησης και προγραμματισμού της λειτουργίας και συντήρησής τους από απόσταση, καθώς και της δυναμικής προσαρμογής του φωτισμού, αποσκοπώντας στην μέγιστη δυνατή ενεργειακή εξοικονόμηση, την ασφάλεια αλλά και την οπτική άνεση των πολιτών.

Τα δεδομένα των «έξυπνων» λύσεων συγκεντρώνονται, μέσω δικτυακών υποδομών, σε Cloud υποδομές του Ομίλου ΟΤΕ και καταλήγουν στην πλατφόρμα Smart & Connected Digital Platform της Cisco. Μέσω της πλατφόρμας γίνεται η διαχείριση των «έξυπνων» λύσεων, καθώς και η ενοποίηση, αποθήκευση και απεικόνιση των δεδομένων από τις εφαρμογές, μέσω ενός ενιαίου περιβάλλοντος προβολής (dashboard). Η Smart & Connected Digital Platform έχει τη δυνατότητα μελλοντικής ενσωμάτωσης περισσότερων έξυπνων λύσεων.

Σύστημα μέτρησης περιβαλλοντικών παραμέτρων για καλύτερη ποιότητα ζωής

Το σύστημα μέτρησης περιβαλλοντικών παραμέτρων, που έχει εγκατασταθεί από τον Όμιλο ΟΤΕ, χρησιμοποιεί αισθητήρες υψηλής ποιότητας για την ανίχνευση επιβλαβών αερίων στην ατμόσφαιρα και τριών τύπων μικροσωματιδίων. Θα μετρά επίσης θερμοκρασία, υγρασία και ατμοσφαιρική πίεση. Έτσι, η Δημοτική Αρχή θα μπορεί να σχεδιάσει

καλύτερα και να υλοποιήσει δράσεις για τη μείωση της ατμοσφαιρικής ρύπανσης, βελτιώνοντας την ποιότητα ζωής των κατοίκων.

3.7.3: Η έξυπνη πόλη στο Ηράκλειο Κρήτης

Το Ηράκλειο συμπεριλαμβάνεται στη λίστα των 100 intelligent cities (Έξυπνες Πόλεις) της Ευρώπης μετά από αξιολόγηση της ψηφιακής πολιτικής του. Η αξιολόγηση έγινε από την πρωτοβουλία Intelligent cities challenge της Ευρωπαϊκής Επιτροπής.

3.7.3.1: Το όραμα της smart city του Ηρακλείου

Ο Δήμος Ηρακλείου είναι ένας από τους πρώτους δήμους της χώρας που προσφέρει ένα σύνολο από 163 ηλεκτρονικές υπηρεσίες στους δημότες του. Οι χρήστες μπορούν να κατεβάσουν τα επίσημα έντυπα, τα συμπληρώνουν και να τα υποβάλουν σε απευθείας σύνδεση ή τα εκτυπώνουν και τα συμπληρώνουν με το χέρι.

- **e-πληρωμές** – για τις πληρωμές των οφειλών προς το Δήμο
- **e-βιβλιοθήκη** – για τη δέσμευση των βιβλίων που πρόκειται να δανειστούν από τη δημόσια βιβλιοθήκη σε απευθείας σύνδεση
- **Βάση δεδομένων των διοικητικών αποφάσεων** – μια ηλεκτρονική βάση δεδομένων όλων των διοικητικών αποφάσεων που λαμβάνονται από τις δημοτικές επιτροπές του δήμου από 01/01/1990 και μετά.
- **Πολεοδομία GIS** – ένα σύστημα GIS για την οργάνωση των δεδομένων του πολεοδομικού σχεδιασμού με σκοπό την ταχύτερη, ευκολότερη και καλύτερη εξυπηρέτηση του πολίτη.

Επικεντρώνουν την προσοχή τους στην ενίσχυση της εστιασμένης προσωπικής εξυπηρέτησης των πολιτών, της βελτίωσης της

διαδραστικότητας, και στην μείωση του κόστους των υπηρεσιών. Η προσωπική εξυπηρέτηση μέσω ΤΠΕ μπορεί να μειώσει το κόστος το υπηρεσιών αλλά ταυτόχρονα να βελτιώσει σημαντικά την ποιότητα τους.

Οι προσπάθειες θα συνεχιστούν τα επόμενα χρόνια ώστε ολοένα και περισσότερες υπηρεσίες να παρέχονται προς τους πολίτες, όπως για παράδειγμα η παροχή υπηρεσιών ηλεκτρονικής πληρωμής Κοινωνικών Παροχών. Έτσι αποφεύγονται οι παραδοσιακές ουρές στις υπηρεσίες και υπάρχει η δυνατότητα εγκαίρων πληρωμών σε αυτούς που το έχουν ανάγκη.

3.7.3.2: Τα έργα που έγιναν στην smart city του Ηρακλείου

Έχουν πραγματοποιηθεί περισσότερα από 30 έργα για την διευκόλυνση των πολιτών στο Ηράκλειο. Μερικά από αυτά είναι:

Εφαρμογή «Φόρτος κίνησης σε δρόμους»:
Πρόκειται για ένα έξυπνο σύστημα μέτρησης του κυκλοφοριακού φόρτου , ενταγμένο στην ψηφιακή πλατφόρμα smartcity.heraklion.gr (https://traffic.smartcity.heraklion.gr/) με σκοπό τη βέλτιστη χρήση των οδικών δικτύων και την καλύτερη εξυπηρέτηση, ασφάλεια και βελτίωση της αποδοτικότητάς τους, με την εισαγωγή πληροφοριακών συστημάτων, εφαρμογών και υπηρεσιών διαδικτύου.

Συγκεκριμένα, το σύστημα τη δεδομένη στιγμή επιτρέπει:

- Την παρουσίαση δυναμικών αποτελεσμάτων , παρέχοντας πληροφόρηση για την κίνηση στη Λεωφόρο Ικάρου σε πραγματικό χρόνο.

- Την παρουσίαση μετρήσεων του κυκλοφοριακού φόρτου για όποιο χρονικό διάστημα επιθυμεί ο ενδιαφερόμενος

• Την παρουσίαση συγκριτικών αποτελεσμάτων κυκλοφοριακού φόρτου (με βάση τον χρόνο)

• Την οπτικοποίηση των δεδομένων κυκλοφοριακού φόρτου, σε πραγματικό χρόνο, στην πλατφόρμα έξυπνης πόλης του Δήμου για περαιτέρω αξιοποίηση τους.

Ψηφιακή επικοινωνία των Δημοτών με την ΔΕΥΑ Ηρακλείου

Με μια νέα mobile εφαρμογή θα μπορούν να επικοινωνούν οι δημότες με την ΔΕΥΑΗ. Η εφαρμογή αναπτύχθηκε για την καλύτερη δυνατή εξυπηρέτηση των δημοτών, ειδικά όσον αφορά στη διαχείριση των βλαβών. Οι δημότες μπορούν να χρησιμοποιήσουν την εφαρμογή και να δηλώσουν βλάβες με δυο τρόπους:

Μέσω Η/Υ (desktop ή laptop), στην παρακάτω ιστοσελίδα: https://platform.cityzenapp.gr/cityzen/deyah

Μέσω της εφαρμογής για κινητές συσκευές, την οποία μπορούν να εγκαταστήσουν στο τηλέφωνό τους από το Play store ή Appstore, πληκτρολογώντας ΔΕΥΑ Ηρακλείου

Ηλεκτρονική εφαρμογή «Δημότης Ηρακλείου» για την εξυπηρέτηση των πολιτών

Μεγάλη απήχηση στους Ηρακλειώτες έχει η ηλεκτρονική εφαρμογή «Δημότης Ηρακλείου» που ανέπτυξε ο Δήμος για την γρήγορη εξυπηρέτησή τους, την καταγραφή των προβλημάτων και την άμεση επίλυσή τους από τις αρμόδιες υπηρεσίες. Στο πλαίσιο αυτό κυκλοφόρησε η ανανεωμένη έκδοση της εφαρμογής για κινητές συσκευές και προσφέρει νέες δυνατότητες. Συνεχίζουμε, δήλωσε ο Δήμαρχος Ηρακλείου κ. Βασίλης Λαμπρινός, την ενίσχυση των πολιτικών Ηλεκτρονικής Διακυβέρνησης με αύξηση των παρεχόμενων υπηρεσιών στους πολίτες, επισκέπτες και

επιχειρήσεις μέσω «έξυπνων» εφαρμογών και για κινητές συσκευές.

«Η εφαρμογή «Δημότης Ηρακλείου» έχει μεγάλη απήχηση στους συμπολίτες. Με τη χρήση της άλλαξε η αναλογία επικοινωνίας των δημοτών με τον Δήμο αφού πριν την εμφάνιση της η υποβολή αιτημάτων μέσω τηλεφώνου ήταν 75% ενώ τώρα 50% των αιτημάτων υποβάλλεται ηλεκτρονικά και 50% τηλεφωνικά» επεσήμανε ο Δήμαρχος .

Ο δημότες μέσω της ηλεκτρονικής εφαρμογής μπορούν:

- Να συνδεθούν μέσω TAXISnet, Google, Facebook ή μέσω της ιστοσελίδας του δήμου.
- Να επιλέξουν τι θα βλέπουν στην αρχική σελίδα σύμφωνα με τα δικά τους ενδιαφέροντα.
- Να δουν το ιστορικό των προβλημάτων που έχουν υποβάλει στο παρελθόν χρησιμοποιώντας τον αριθμό τηλεφώνου που είχαν δώσει κατά την υποβολή.
- Να συνδεθούν μέσω TAXISnet και αιτηθούν πιστοποιητικά από το κινητό τους.
- Να δουν πληροφορίες Πολιτικής Προστασίας σε περίπτωση έκτακτου γεγονότος με offline χάρτες και οδηγίες προστασίας.

3.8: Έξυπνες πόλεις ανά τον κόσμο

3.8.1: Η έξυπνη πόλη της Σιγκαπούρης

Τη δεύτερη θέση στο “top 5” των πιο “έξυπνων” πόλεων του πλανήτη για το 2022 κατακτά η Σεούλ, η Βαρκελώνη κατατάσσεται 3η, ενώ ακολουθούν το Πεκίνο και η Νέα Υόρκη. Η Juniper Research αναδεικνύει μέσα από την έρευνα της τις 50 πιο “έξυπνες” πόλεις, παγκοσμίως, αξιολογώντας μια σειρά από κριτήρια.

Μία «έξυπνη», οικολογική πόλη, με 42.000 κατοικίες κατασκευάζεται στη Σιγκαπούρη.

Η Tengah θα είναι ο πέμπτος οικισμός που κατασκευάζει η κυβέρνηση της χώρας από τον Β' Παγκόσμιο Πόλεμο, αλλά θα είναι η πρώτη με κεντρικό κλιματισμό, αυτόματη διακομιδή απορριμμάτων και κέντρο χωρίς αυτοκίνητα.

Η πόλη, που θα διαθέτει άφθονο πράσινο και δημόσιους κήπους, θα καταλάβει περιοχή 7 τετραγωνικών χιλιομέτρων που κάποτε φιλοξενούσε εργοστάσια παραγωγής τούβλων, στη συνέχεια χρησιμοποιήθηκε για στρατιωτική εκπαίδευση και τώρα έχει μετατραπεί σε δάσος.

Στο κέντρο της θα διατηρηθεί ένας οικολογικός «διάδρομος», μήκους 100 μέτρων, που θα παρέχει ασφαλή διέλευση σε άγρια ζώα και θα συνδέει περιοχή απορροής υδάτων από τη μια μεριά και ένα καταφύγιο άγριας ζωής από την άλλη.

Οι δρόμοι και οι χώροι στάθμευσης θα είναι υπόγειοι.

Στην πόλη θα εγκατασταθούν σταθμοί φόρτισης ηλεκτρικών οχημάτων, ενώ οι δρόμοι σχεδιάστηκαν με το βλέμμα στο μέλλον και τις νέες τεχνολογίες που αυτό θα φέρει.

Αν και έχει πληθυσμό μικρότερο των 6 εκατομμυρίων, οι κατά κεφαλήν εκπομπές διοξειδίου άνθρακα της Σιγκαπούρης είναι μεγαλύτερες από εκείνες της Βρετανίας, της Κίνας και της Μαλαισίας. Κάτι που σε ένα βαθμό οφείλεται και στα κλιματιστικά.

Οι σχεδιαστές της «έξυπνης» πόλης επέλεξαν έναν διαφορετικό τρόπο κλιματισμού. Νερό, που θα ψύχεται με τη χρήση ηλιακής ενέργειας, θα περνά μέσω σωλήνων από τα σπίτια, κάτι που σημαίνει ότι οι κάτοικοι δεν θα χρειάζονται εξωτερικές μονάδες κλιματισμού. Πάντως, θα μπορούν να ελέγξουν τη θερμοκρασία του διαμερίσματός τους.

Σύμφωνα με την SG Group, τον πάροχο ενέργειας της πόλης, αυτό το σύστημα θα οδηγήσει σε μείωση εκπομπών διοξειδίου του άνθρακα που ισοδυναμεί με την απόσυρση 4.500 αυτοκινήτων από τους δρόμους κάθε χρόνο.

Επίσης, στους δημόσιους χώρους θα υπάρχουν «έξυπνα» φώτα που θα σβήνουν όταν δεν βρίσκεται κόσμος εκεί, ενώ τα σκουπίδια θα αποθηκεύονται κεντρικά και μόνιτορ θα ανιχνεύουν πότε πρέπει να γίνει διακομιδή.

Επίσης όλοι οι κάτοικοι θα έχουν πρόσβαση σε εφαρμογή που θα τους επιτρέπει να παρακολουθούν την κατανάλωση ενέργειας και νερού, ώστε να μπορούν να αποφασίσουν οι ίδιοι που θα κάνουν περικοπές. Παράλληλα, ψηφιακές «πινακίδες» σε κάθε συγκρότημα θα ενημερώνουν τους κατοίκους για το συλλογικό αποτύπωμα στο περιβάλλον, κάτι που- σύμφωνα με την SP Group- μπορεί να οδηγήσει και σε ανταγωνισμό ανάμεσα σε συγκροτήματα.

3.8.2: Η έξυπνη πόλη της Σεούλ στη Νότια Κορέα

Στην βιομηχανική συνοικία της Σεούλ, ειδικοί και αρχές οραματίζονται μία έξυπνη πόλη για την ψηφιακή οικονομία, όπου η καινοτομία και η διαφορετικότητα δημιουργούν έναν ελκυστικό χώρο διαμονής, εργασίας και ψυχαγωγίας.

Το σκηνικό συνθέτουν χώροι πρασίνου δίπλα σε πεζόδρομους και τεράστιες κατασκευές -δημόσιες, ημιδημόσιες και ιδιωτικές- με ψηφιακά εξυπηρετούμενες υποδομές, για έλεγχο της κατανάλωσης πράσινης ενέργειας και της διαχείρισης της παραγωγής σε κοινόχρηστους χώρους, που θα περιλαμβάνουν αστικές φάρμες και συστήματα συλλογής και αποθήκευσης της βρόχινου νερού για συνετή χρήση.

3.8.3: Η έξυπνη πόλη της Βαρκελώνης

Στην κορυφή των έξυπνων πόλεων βρίσκεται η Βαρκελώνη, όπου στους δρόμους της πόλης υπάρχει ο έξυπνος φωτισμός: τα φώτα LED που διαθέτουν αισθητήρες μπορούν να ανιχνεύσουν την κίνηση, τον καιρό, τη ρύπανση και τον θόρυβο.

Τα φώτα μπορούν να ελέγχονται εξ αποστάσεως, να ενεργοποιούνται ή να απενεργοποιούνται. Επίσης, με αισθητήρες κίνησης μπορούν να προσφέρουν ρύθμιση φωτεινότητας όταν δεν υπάρχει κίνηση, για περαιτέρω εξοικονόμηση ενέργειας.

Τα δεδομένα από τους αισθητήρες μπορούν να βοηθήσουν στον εντοπισμό αυξημένης κυκλοφοριακής κίνησης καθώς και στη βελτίωση της ασφάλειας.Σε πλήρη ανάπτυξη υπάρχει και το έξυπνο parking: ανιχνευτές εικόνας και μετάλλων εγκατεστημένοι σε κάθε θέση στάθμευσης του δρόμου γνωρίζουν, εάν ο χώρος είναι κατειλημμένος. Οι οδηγοί λαμβάνουν πληροφορίες σε πραγματικό χρόνο, σχετικά με τις διαθέσιμες θέσεις στάθμευσης χρησιμοποιώντας μία mobile εφαρμογή στο κινητό τους τηλέφωνο.

Η ανάλυση των δεδομένων που παράγονται από αυτό το έξυπνο σύστημα, βοηθούν την πόλη να σχεδιάσει καλύτερους δρόμους και χώρους στάθμευσης. Οι εφαρμογές δημόσιας ασφάλειας περιλαμβάνουν την παρακολούθηση των πιο επικίνδυνων σημείων της πόλης και χάρτη καθημερινής εγκληματικότητας. Στην πόλη λειτουργούν 110 δημόσιοι σταθμοί φόρτισης ηλεκτρικών οχημάτων. Οι δικτυωμένοι σταθμοί επιτρέπουν στην πόλη να παρακολουθεί τη χρήση και την κατάσταση των φορτιστών. Οι χρήστες συνδέονται σε ειδική εφαρμογή για να βρουν τον πλησιέστερο σταθμό και να παρακολουθήσουν τα στατιστικά στοιχεία χρήσης.

Κεφάλαιο 4: Η ασφάλεια στις Smart Cities

Η ασφάλεια είναι ένα ακόμα κρίσιμο θέμα στο πλαίσιο των Έξυπνων Πόλεων (Smart Cities). Καθώς οι Έξυπνες Πόλεις εξαρτώνται από τεχνολογία και δίκτυα για τη βελτίωση της ποιότητας ζωής, την ασφάλεια των πολιτών και την αποτελεσματικότητα των υπηρεσιών, είναι σημαντικό να δίνεται έμφαση στα θέματα ασφάλειας.

Για να διασφαλιστεί η ασφάλεια στις Έξυπνες Πόλεις, απαιτείται η συνεργασία μεταξύ των κυβερνήσεων, των επιχειρήσεων, των ειδικών στην κυβερνοασφάλεια και των πολιτών. Πρέπει να δοθεί προσοχή στην ανάπτυξη ασφαλών τεχνολογικών λύσεων, στην εκπαίδευση των πολιτών για την κυβερνοασφάλεια και στη συνεχή παρακολούθηση και βελτίωση των συστημάτων ασφαλείας των Έξυπνων Πόλεων.

4.1 Σημασία της Ασφάλειας στις Έξυπνες Πόλεις

Η ασφάλεια για τις έξυπνες πόλεις αναφέρεται σε ένα μεγαλύτερο πρόβλημα και δεν πρέπει να το αντιλαμβανόμαστε απομονωμένα. Με τον όρο "απομονωμένα", αναφερόμαστε στην ανάπτυξη λύσεων ασφαλείας για συγκεκριμένες εφαρμογές έξυπνης πόλης, όπως έξυπνη μεταφορά, έξυπνη υγεία, έξυπνο περιβάλλον, έξυπνη ζωή. Αντίθετα, πρέπει να κατανοήσουμε και να αναλύσουμε τους υποκείμενους παράγοντες που θα διέπουν και θα συνεισφέρουν στην ασφάλεια της λειτουργίας και των υπηρεσιών αυτών των εφαρμογών μιας έξυπνης πόλης.

Αποτελεσματικά, χρειάζεται να ασφαλίσουμε το "μυαλό", το "σώμα" και τις "αισθήσεις" μιας έξυπνης πόλης, εκτός της ασφάλειας κάθε εφαρμογής της έξυπνης πόλης. Αυτό απαιτεί μια συνολική και ολοκληρωμένη λύση ασφαλείας για την προστασία μιας έξυπνης πόλης. Όπως φαίνεται στο ακόλουθο σχήμα, η λύση ασφαλείας δεν θα προστατεύσει μόνο την πόλη από επιθέσεις από εισβολείς εκτός της πόλης, αλλά θα προστατεύσει επίσης την εσωτερική της δομή, την συνδεσιμότητα, τις εφαρμογές και τις υπηρεσίες που εμπεριέχονται σε αυτή.

Εικόνα 8 Η ασπίδα προστασίας και ασφάλειας μιας έξυπνης πόλης ισοδυναμεί με την ύπαρξη πολλαπλών επιπέδων προστασίας ασφαλείας, από την προστασία του εγκεφάλου μέχρι τις αισθήσεις και το σώμα.

4.2 Προκλήσεις για την Ασφάλεια στις έξυπνες πόλεις

4.2.1: Θέματα κινδύνου στην επεξεργασία και διαχείριση δεδομένων

Πολλά άγνωστα πηγάζουν από τη διαχείριση και επεξεργασία δεδομένων στο Διαδίκτυο των πραγμάτων, με άμεση επίδραση στην ανθεκτικότητα και στη σταθερότητα των οικοσυστημάτων. Όπως αναφέρεται στην ακόλουθη φράση: "Η ασφάλεια είναι δύσκολη. Ακόμα και σε μικρούς οργανισμούς με καλά κατανεμημένες υποδομές δικτύου, δεν μπορεί να εγγυηθεί η αποτροπή των εισβολέων. Φανταστείτε μια μεγάλη, ποικίλη υποδομή όπου διάφορες γραφειοκρατίες και συστατικά κρίσιμης υποδομής μοιράζονται πολύπλοκες αλληλεπιδράσεις με, ίσως, καμία συνολική κυβερνοασφαλή αρχιτεκτονική. Αυτό είναι πιθανώς το πρόβλημα που αντιμετωπίζει η πόλη σας." Αυτή η αβεβαιότητα δημιουργεί μια ποικιλία κινδύνων που πρέπει να αναγνωριστούν και να διαχειριστούν μέσω μιας διαδικασίας διαχείρισης κινδύνων για να εξασφαλιστεί μια ασφαλής ανάπτυξη των πόλεων. Γι' αυτό το σκοπό, οι υπάρχουσες προδιαγραφές και μεθοδολογίες θα μπορούσαν να προσαρμοστούν στις συγκεκριμένες ανάγκες, τα πλαίσια και τις πολυπλοκότητες των πόλεων, των κοινοτήτων και των έργων. Ανάμεσα σε αυτούς τους κινδύνους, η ιδιωτικότητα και η ασφάλεια αποτελούν

σημαντική απειλή. Ωστόσο, όπως φαίνεται στην εικόνα 9, ένα νέο παράδειγμα απαιτεί την ταχύτερη εφαρμογή μιας δυναμικής προσέγγισης διαχείρισης κινδύνων, ικανής να προβλέπει κινδύνους και απειλές μέσω μιας συνεχούς διαδικασίας.

Αποφάσεις βασισμένες σε δεδομένα

Οι έξυπνες πόλεις εμπεριέχουν έναν αυξανόμενο αριθμό αποφάσεων που βασίζονται σε δεδομένα σχετικά με μια ευρεία γκάμα θεμάτων (ενέργεια, κίνηση, φόροι, ασφάλεια, ασφάλιση, κλπ.) και εμπλεκόμενα μέρη (πολίτες, πόλεις, εταιρείες, κλπ.), ελπίζοντας για αποτελεσματικές, δίκαιες και αμερόληπτες αποφάσεις που θα οδηγήσουν σε λειτουργική αποτελεσματικότητα, βιώσιμη οικονομική ανάπτυξη και κοινωνική δικαιοσύνη. Η αποτελεσματικότητα της διαδικασίας λήψης αποφάσεων εξαρτάται από τεχνικούς και μη τεχνικούς παράγοντες, όπως αλγόριθμοι, ποιότητα δεδομένων και διακυβέρνηση - καθένας από τους οποίους μπορεί να αποτελέσει πηγή προκατάληψης ή λάθους. Ποιες, λοιπόν, είναι οι οικονομικές, κοινωνικές ή περιβαλλοντικές συνέπειες των λανθασμένων αποφάσεων, προκαταλήψεων ή λαθών λόγω κακής ποιότητας δεδομένων, παρανόησης ή ανικανότητας χρήσης των δεδομένων με αποτελεσματικό τρόπο;

Νέα επιχειρηματικά μοντέλα

Τα επιχειρηματικά μοντέλα ενός αυξανόμενου αριθμού εταιρειών βασίζονται στα δεδομένα. Μπορούμε λοιπόν να αναρωτηθούμε εάν αυτά τα επιχειρηματικά μοντέλα είναι ανθεκτικά στα προβλήματα δεδομένων και στην αβεβαιότητα που σχετίζεται με νέες τεχνολογίες (blockchain, AI...), εάν οι δεξιότητες των ανθρώπων (πολίτες, δημόσιοι υπάλληλοι, εργαζόμενοι σε επιχειρήσεις...) προσαρμόζονται στις πραγματικές και μελλοντικές ανάγκες που προκαλεί η ψηφιοποίηση, και γενικότερα, εάν η εταιρική διακυβέρνηση προσαρμόζεται στον μεταβαλλόμενο οικονομικό κόσμο;

Η ψηφιοποίηση δημιουργεί επίσης προκλήσεις στα μοντέλα αξιολόγησης που διαμορφώνουν την εταιρική χρηματοοικονομική. Είναι τα

επιχειρηματικά μοντέλα και οι αξιολογήσεις ανθεκτικές σε αυτήν τη νέα εποχή της τεχνολογίας;

Ποιες είναι οι συνέπειες στα μοντέλα επιχειρήσεων και στην αξία τους λόγω λανθασμένων αποφάσεων; Ποιες είναι οι συνέπειες λόγω κακής ποιότητας δεδομένων και αδυναμίας σωστής χρήσης των δεδομένων; Ποιες είναι οι συνέπειες των προβλημάτων δεδομένων στη σχέση με τον πελάτη και το κύρος; Είναι οι εταιρείες σε θέση να διατηρήσουν υψηλές δυνατότητες αναφοράς / ικανότητας κατανόησης των δραστηριοτήτων τους μέσα στον διασυνδεδεμένο περιβάλλον που δημιουργείται από έξυπνες πόλεις και το Διαδίκτυο των Πραγμάτων;

Επιπλέον, η πραγματική συγκέντρωση της παγκόσμιας οικονομίας γύρω από ένα περιορισμένο αριθμό υπηρεσιών, υλικού και παροχών τεχνολογίας θέτει τα ερωτήματα του κινδύνου συγκέντρωσης και των τεχνολογικών και δεδομένων εξαρτημάτων. Για παράδειγμα, ποιες θα μπορούσαν να είναι οι επιπτώσεις μιας μαζικής διακοπής ρεύματος (ηλεκτρικό ρεύμα, μεταφορές, τραπεζικό σύστημα κ.λπ.), εμποδίου που προκύπτει από οικονομικό ανταγωνισμό ή πτώχευσης ενός μεγάλου παρόχου υπηρεσιών. Οι απαντήσεις σε βασικά ερωτήματα όπως "πότε θα επανέλθουν τα πράγματα στο φυσιολογικό;", "τι συμβαίνει κατά τη διάρκεια μιας διακοπής ρεύματος για να διατηρηθεί μία δραστηριότητα;", ή "μπορούμε ακόμα να λειτουργήσουμε με παλιά συστήματα;" θα πρέπει να προβλεφθούν.

Τέλος, η τρέχουσα οικονομική πίεση μπορεί να δημιουργήσει απρόβλεπτο μέλλον για τον παράγοντα του κόστους. Όπως δηλώνεται ήδη, "είναι επικίνδυνο να θεωρούμε αυτές τις γρήγορες επιτυχίες ως δωρεάν". Αυτό μας ενθαρρύνει να θεωρήσουμε το κόστος της τεχνολογίας ως έναν κίνδυνο.

Νέα σύνορα του δικαίου

Νομικά θέματα προκαλούνται από την επεξεργασία και διαχείριση δεδομένων στο Διαδίκτυο των Πραγμάτων, σε ένα πλαίσιο διάφορων ενδιαφερόμενων μερών (δημόσιου/ιδιωτικού τομέα, ανάμεσα σε διάφορες πόλεις/πολίτες, εταιρείες...) και προηγμένων τεχνολογιών (μεταφορά δεδομένων, cloud κλπ.):

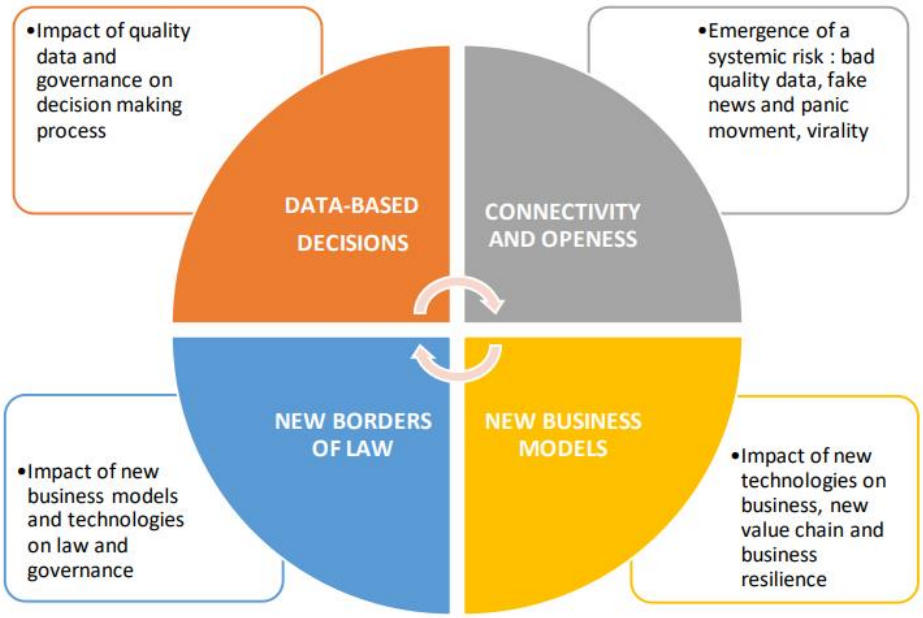
- Θέματα δικαιοδοσίας που σχετίζονται με το νομικό πλαίσιο επεξεργασίας και αποθήκευσης δεδομένων στο δημόσιο/ιδιωτικό νέφος (cloud), μεταφορά δεδομένων και διασυνοριακές ροές.
- Νομικά και διοικητικά θέματα που σχετίζονται με την ιδιοκτησία των δεδομένων, την προστασία των δεδομένων, την άνετη μεταφορά των δεδομένων μεταξύ παρόχων υπηρεσιών νέφους (π.χ. φορητότητα αριθμών κινητών τηλεφώνων).
- Πραγματικός χρόνος επεξεργασίας (5G, πραγματική χρονική ανάλυση.) που παράγει μια επιτάχυνση των αποφάσεων που μπορούν τώρα να ληφθούν αμέσως μέσω της εκχώρησης αποφάσεων σε αλγόριθμους και μηχανές. Αυτό θέτει ερωτήματα σχετικά με την ηθική των αλγορίθμων, τον έλεγχο, και την αξιοπιστία.

Συνδεσιμότητα

Το γεγονός ότι οι Έξυπνες Πόλεις και το Διαδίκτυο των Πραγμάτων (IoT) χαρακτηρίζονται από τη χρήση "δεδομένων για τα πάντα" και ότι συσκευές, αντικείμενα, εργαλεία, αισθητήρες, εργαλεία παρακολούθησης (...) μπορούν να είναι ανοιχτά και/ή συνδεδεμένα με άλλες συσκευές, εργαλεία, συστήματα (...) δημιουργούν τεράστιες ροές δεδομένων και ανταλλαγές δεδομένων. Αυτό το πολύ υψηλό επίπεδο συνδεσιμότητας μπορεί να δημιουργήσει μια ιογενή απειλή: μετάδοση δεδομένων χαμηλής ποιότητας, διάδοση εσφαλμένων πληροφοριών που οδηγούν σε πανικό, ή διάδοση ψευδών ειδήσεων.

Σε υψηλότερο επίπεδο, ένα απομονωμένο πρόβλημα μπορεί να οδηγήσει σε μαζικό, με γενικό αποτέλεσμα σε ολόκληρο το οικοσύστημα, δημιουργώντας ένα Συστημικό κίνδυνο.

Μια ενδιαφέρουσα προοπτική θα μπορούσε να είναι η μετάφραση ενός τέτοιου κινδύνου στο περιβάλλον των Έξυπνων Πόλεων και του Διαδικτύου των Πραγμάτων, όπου οι διασυνδέσεις, οι ροές δεδομένων, η αμοιβαία χρήση υπηρεσιών, συσκευών ή πηγών ενέργειας μπορούν να προκαλέσουν τη μετάδοση προβλημάτων και αποτυχιών.



Εικόνα 9 Οι κίνδυνοι που δημιουργούνται από τις Έξυπνες Πόλεις και το συγκεκριμένο πλαίσιο του Διαδικτύου των Πραγμάτων

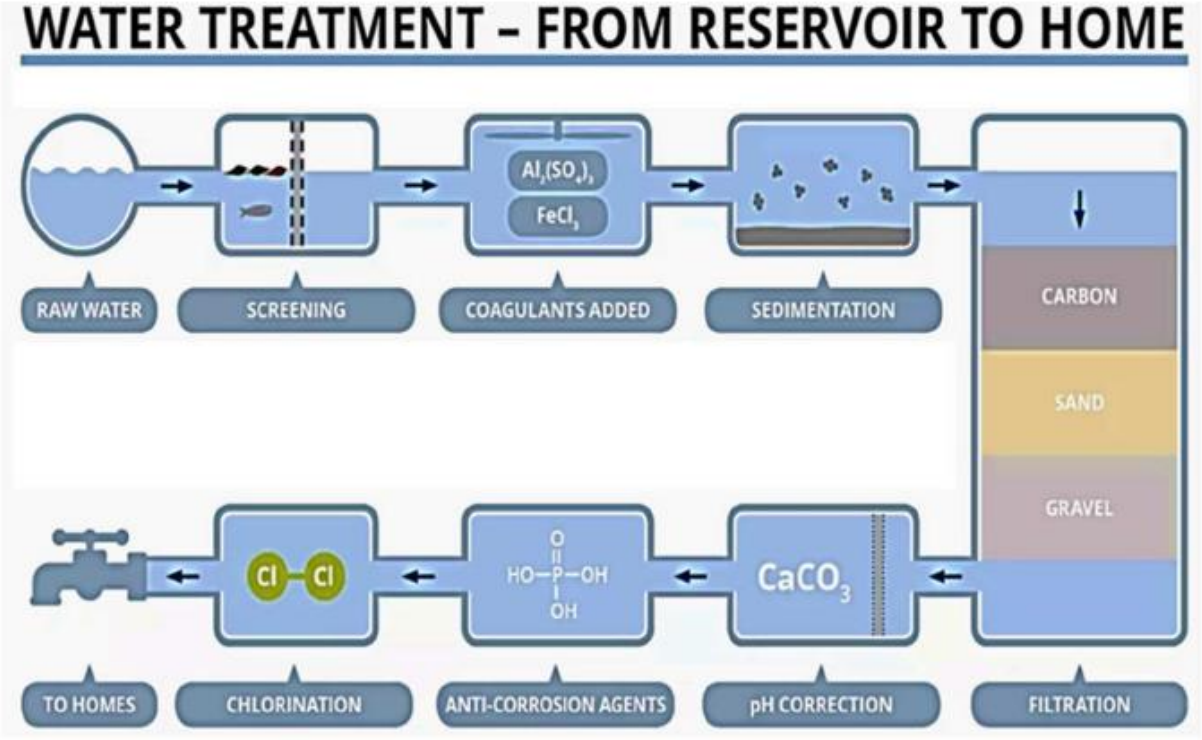
Μόλις περιγράψαμε, τους κινδύνους που προκύπτουν από την επεξεργασία και διαχείριση δεδομένων στο Διαδίκτυο των Πραγμάτων και τις Έξυπνες Πόλεις , και όπως είδαμε είναι πολλοί και ποικίλοι. Περιλαμβάνουν κινδύνους απόρρητου και ασφάλειας, αλλά επίσης και πολλούς άλλους κρίσιμους κινδύνους που πηγάζουν από την τεράστια χρήση δεδομένων παντού και σε κάθε στάδιο της χρήσης των Έξυπνων Πόλεων και του Διαδικτύου των Πραγμάτων. Η πιθανότητα εμφάνισης και η έκταση τέτοιων κινδύνων πρέπει να αξιολογηθούν, και οι ευθύνες πρέπει να διευκρινιστούν σε περίπτωση εμφάνισης, προκειμένου να καθοριστεί ποιος κατέχει τους κινδύνους και τελικά να επιβαρυνθούν τα κόστη της αβεβαιότητας.

4.3 Τομείς που χρήζουν ασφάλειας στις έξυπνες πόλεις

4.3.1: Διασφάλιση παροχής νερού

Ένα ουσιώδες στοιχείο για την επιβίωση του ανθρώπου είναι το νερό, και γι' αυτό είναι υψηλότερης προτεραιότητας. Μια πόλη δεν μπορεί να συνεχίσει την κανονική της ζωή χωρίς την παρουσία νερού, τόσο για προσωπική κατανάλωση όσο και για επιχειρήσεις (σε εστιατόρια κλπ.). Οι επιθέσεις σε πηγές νερού αλλά και σε μεταφορές νερού μπορούν να διαταράξουν τον εφοδιασμό νερού. Τέτοιες επιθέσεις μπορούν να γίνουν φυσικά από τους επιτιθέμενους στις υποδομές νερού, αποσυνδέοντας αντλίες ισχύος και σπάζοντας σωλήνες μεταφοράς νερού στην αλυσίδα εφοδιασμού. Οι επιθέσεις που γίνονται στις υποδομές αυτές συνήθως αποτρέπονται από την παρουσία ατόμων ασφαλείας και επιτήρησης μέσω βίντεο στις διάφορες υποδομές. Ωστόσο, ψηφιακές επιθέσεις που διεξάγονται από επιτιθέμενους που βρίσκονται απομακρυσμένα (έξω από την πόλη) μπορεί να είναι δύσκολο να αντιμετωπιστούν. Μέσω του κυβερνοχώρου, αποκτούν έλεγχο επί του συστήματος διαχείρισης του νερού για να το απενεργοποιήσουν ή να μειώσουν την παροχή νερού στην πόλη. Τα προγράμματα ελέγχου πρέπει να είναι παρόντα 24 ώρες το 24ωρο για να παρακολουθούν συνεχώς για «ανωμαλίες» και η απομακρυσμένη πρόσβαση στο σύστημα διαχείρισης του νερού πρέπει να περιορίζεται σε λίγους ή ακόμα και να απαγορεύεται.

Η μόλυνση του νερού είναι ένα κρίσιμο γεγονός που πρέπει να αποφευχθεί. Οι επιτιθέμενοι μπορούν να καταφύγουν στη δηλητηρίαση του ύδατος που προορίζεται για πόσιμο νερό για να μολύνουν γρήγορα εκατομμύρια ανθρώπους, με αποτέλεσμα να αρρωστήσουν ή να πεθάνουν. Στις Ηνωμένες Πολιτείες, ο Νόμος Βιοτρομοκρατίας (2002) αποτελεί ένα νομικό πλαίσιο για την αντιμετώπιση αυτού του ζητήματος. Ο Νόμος Βιοτρομοκρατίας απαιτεί από τις υπηρεσίες πόσιμου νερού που εξυπηρετούν περισσότερους από 3300 ανθρώπους να διενεργούν αξιολογήσεις ευπάθειας και να αναπτύσσουν σχέδια έκτακτης αντίδρασης. Όπως φαίνεται στην εικόνα 10, με την παρεμβολή σε οποιοδήποτε μέρος της διαδικασίας επεξεργασίας και παροχής νερού, μπορεί κανείς να μολύνει την παροχή νερού με χημικούς κινδύνους.



Εικόνα 10 Η παροχή νερού περιλαμβάνει την επεξεργασία του νερού πριν από την παράδοση του στην βρύση

4.3.2: Διασφάλιση ενέργειας

Η πλειονότητα των εφαρμογών , που βρίσκονται εντός των έξυπνων πόλεων σήμερα τροφοδοτούνται από ηλεκτρισμό. Χωρίς ενέργεια, η πλειονότητα του συστήματος μίας έξυπνης πόλης και των επιχειρήσεων θα σταματήσουν να λειτουργούν και η πόλη θα μείνει στο σκοτάδι. Ως εκ τούτου, η ασφάλεια της πηγής ενέργειας και της διανομής ενέργειας είναι κρίσιμη για τις έξυπνες πόλεις. Η παραγωγή ενέργειας μπορεί να διακοπεί με φυσική καταστροφή του χώρου ή διακοπή της διαδικασίας παραγωγής ηλεκτρισμού. Αυτό απαιτεί αυστηρή ασφάλεια του χώρου για να διασφαλιστεί ότι η παραγωγή ενέργειας δεν θα διακοπεί και ότι υπάρχει αντίγραφο ασφαλείας ενέργειας σε περίπτωση διακοπής. Ωστόσο, η παράδοση ενέργειας αναφέρεται στην ενέργεια που μεταφέρεται μέσω γραμμών μεταφοράς ενέργειας, μετασχηματιστών, ρελέ, διακοπτών και κεντρικών σταθμών ενέργειας. Έτσι, επιθέσεις σε

οποιοδήποτε από αυτά τα στοιχεία μπορούν να διακόψουν την παροχή ενέργειας, κάνοντας αναποτελεσματικές όλες τις εφαρμογές έξυπνης πόλης. Πράγματι, έχει αναφερθεί ότι επιτιθέμενοι στόχευαν τους χώρους παραγωγής ενέργειας ως πιθανούς τόπους επίθεσης για να δημιουργήσουν μαζικά blackout σε ολόκληρη την πόλη και πιθανώς να οδηγήσουν σε διαδηλώσεις στους δρόμους. Είναι σημαντικό να θεσπιστεί μια συνολική στρατηγική και ένα πλαίσιο για να διασφαλιστεί τόσο η παραγωγή ενέργειας όσο και η διανομή της ενέργειας στην πόλη. Επιπλέον, καθώς ένα σύστημα ενεργειακής υποδομής είναι υψηλά δικτυωμένο, υπάρχει πιθανότητα για μια σειρά διακοπών, πολλαπλασιάζοντας τον αντίκτυπο μιας μεμονωμένης τοπικής επίθεσης. Αυτό μπορεί να οδηγήσει σε μαζικά blackout σε πολλές πόλεις. Οι έξυπνες πόλεις πρέπει να έχουν ενσωματωμένη ανθεκτικότητα και ικανότητα απομόνωσης για να αντιμετωπίσουν τέτοιου είδους επιθέσεις.

4.3.3: Διασφάλιση συνδεσιμότητας

Οι υποδομές έξυπνων πόλεων απαιτούν συνδεσιμότητα για να συνδέσουν αισθητήρες, κάμερες, κέντρα δεδομένων κλπ. Επομένως, η συνδεσιμότητα είναι η άλλη "φλέβα" (πέραν της ενέργειας) για τις έξυπνες πόλεις. Η συνδεσιμότητα μπορεί να πραγματοποιηθεί μέσω ενσύρματων και ασύρματων δικτύων. Η ασφάλεια του IoT περιλαμβάνει την ασφάλεια της συσκευής, των δεδομένων και της σύνδεσης. Η ασφάλεια της συσκευής περιλαμβάνει την διασφάλιση του απορρήτου της πληροφορίας, τον έλεγχο πρόσβασης και πιστοποίησης. Η ασφάλεια των δεδομένων επιτυγχάνεται μέσω της κρυπτογράφησης ενώ η ασφάλεια της σύνδεσης πραγματοποιείται με τη χρήση πρωτοκόλλων μεταφοράς ασφαλείας από άκρο σε άκρο. Για μια έξυπνη πόλη, οι απαιτήσεις ασφάλειας θα πρέπει να είναι υψηλότερες επειδή οι άνθρωποι περιμένουν μια έξυπνη πόλη να είναι πιο ασφαλής από τις κανονικές πόλεις. Η εικόνα 11 παρουσιάζει μια λίστα μεθόδων προστασίας

ασφάλειας για διάφορους τύπους ασύρματων συνδέσεων, οι οποίες θα συζητηθούν παρακάτω.

Type of wireless links	Security protection methods
• WiFi	WEP and WPA
• Bluetooth	authentication; confidentiality; authorisation [13]
• LORA	See [14, 15]
• SIGFOX	firewall; anti-eavesdropping; authentication; replay avoidance. See [16]
• LTE	see the guide to LTE security [17]. Security mechanisms include authentication, cryptographic protection mechanisms, hardware protection mechanisms, and network protections.

Εικόνα 11 Λίστα ασύρματων συνδέσεων και αντίστοιχων μεθόδων προστασίας ασφαλείας

Ασφάλεια WiFi: Η ασφάλεια των ασύρματων δικτύων απαιτεί την ασφάλεια του ασύρματου συνδέσμου. Απαιτεί ένα πρωτόκολλο ελέγχου πρόσβασης πολυμέσων (MAC) όπου η πρόσβαση στο σύνδεσμο θα ελέγχεται. Στο WiFi, η προστατευμένη πρόσβαση WiFi (WPA) αναπτύχθηκε από το Wi-Fi Alliance για να παρέχει πιο εξελιγμένη δυνατότητα κρυπτογράφησης δεδομένων και καλύτερης αυθεντικοποίησης του χρήστη από την ασύρματη προστασία εμβέλειας (WEP), η οποία ήταν το αρχικό πρότυπο ασφάλειας για WiFi.

Η ασφάλεια του Bluetooth: Το Bluetooth προσφέρει αρκετούς τρόπους ασφάλειας. Σε σχεδόν όλες τις περιπτώσεις, οι χρήστες Bluetooth μπορούν να δημιουργήσουν συσκευές που «εμπιστεύονται» που μπορούν να ανταλλάξουν δεδομένα χωρίς να ζητούν άδεια. Όταν

οποιαδήποτε άλλη συσκευή προσπαθεί να δημιουργήσει σύνδεση με τη συσκευή του χρήστη, ο χρήστης πρέπει να αποφασίσει εάν θα το επιτρέψει. Η ασφάλεια σε επίπεδο υπηρεσίας και σε επίπεδο συσκευής συνεργάζονται για να προστατεύσουν τις συσκευές Bluetooth από μη εξουσιοδοτημένη μετάδοση δεδομένων. Οι μέθοδοι ασφαλείας περιλαμβάνουν διαδικασίες εξουσιοδότησης και αναγνώρισης που περιορίζουν τη χρήση των υπηρεσιών Bluetooth στον εγγεγραμμένο χρήστη και απαιτούν από τους χρήστες να λάβουν μια συνειδητή απόφαση όταν ανοίγουν ένα αρχείο ή αποδέχονται μια μεταφορά δεδομένων. Όσον αφορά αυτά τα μέτρα είναι ενεργοποιημένα στο τηλέφωνο ή σε άλλες συσκευές του χρήστη, είναι απίθανο να συμβεί μη εξουσιοδοτημένη πρόσβαση. Ένας χρήστης μπορεί επίσης απλά να αλλάξει τη λειτουργία Bluetooth του σε "μη εντοπίσιμη" και, επομένως, να αποφύγει πλήρως τη σύνδεση με άλλες ανασφαλείς συσκευές Bluetooth.

Ασφάλεια LORAWAN: Ο σχεδιασμός ασφάλειας του LoRaWAN προσαρμόζεται σε πρωτοποριακές αρχές: η χρήση τυποποιημένων, και καλά δοκιμασμένων αλγορίθμων και η ασφάλεια end-to-end. Η ασφάλεια του LoRaWAN περιλαμβάνει:

(α) αμοιβαία πιστοποίηση

(β) προστασία ακεραιότητας

(γ) εμπιστευτικότητα.

Η αμοιβαία πιστοποίηση καθιερώνεται μεταξύ μιας συσκευής LoRaWAN και του δικτύου LoRaWAN ως μέρος της διαδικασίας σύνδεσης στο δίκτυο. Αυτό εξασφαλίζει ότι μόνο γνήσιες και εξουσιοδοτημένες συσκευές θα ενταχθούν σε γνήσια και αυθεντικά δίκτυα. Τα μηνύματα μέσω του MAC και του LoRaWAN είναι προστατευμένα από παραβίαση ακεραιότητας, προστατευμένα από επαναληπτικές επιθέσεις και

κρυπτογραφημένα. Αυτή η προστασία, σε συνδυασμό με την αμοιβαία πιστοποίηση, εξασφαλίζει ότι η κίνηση στο δίκτυο δεν έχει τροποποιηθεί, προέρχεται από γνήσια συσκευή και δεν είναι κατανοητή από επιτιθέμενους. Η ασφάλεια του LoRaWAN επιπλέον εφαρμόζει κρυπτογράφηση end-to-end για τα αιτήματα εφαρμογών που ανταλλάσσονται μεταξύ των τερματικών συσκευών και των διακομιστών εφαρμογών. Η ασφάλεια του LoRaWAN χρησιμοποιεί το προηγμένο πρωτόκολλο κρυπτογράφησης Advanced Encryption Standard (AES) σε συνδυασμό με διάφορες λειτουργίες λειτουργίας: CMAC2 για προστασία της ακεραιότητας και CTR3 για κρυπτογράφηση. Κάθε συσκευή LoRaWAN προσαρμόζεται με ένα μοναδικό κλειδί AES 128 bit (που ονομάζεται AppKey) και ένα παγκοσμίως μοναδικό αναγνωριστικό (EUI-64-based DevEUI), τα οποία χρησιμοποιούνται κατά τη διαδικασία πιστοποίησης της συσκευής.

Ασφάλεια SIGFox: Το SIGFox είναι μια λύση χαμηλής κατανάλωσης ενέργειας και χαμηλού κόστους για τη σύνδεση αισθητήρων και συσκευών. Η ραδιοεπικοινωνία μεταξύ των βάσεων και του cloud SIGFox, καθώς και το ίδιο το cloud SIGFox, ασφαλίζονται χρησιμοποιώντας αυθεντικοποίηση με βάση υπογραφές και εικονικό ιδιωτικό δίκτυο (VPN). Οι χρήστες συνδέονται με το cloud SIGFox χρησιμοποιώντας ασφαλές πρωτόκολλο μεταφοράς (HTTPS) για κρυπτογραφημένες διεπαφές. Το SIGFox διαθέτει ενσωματωμένο τείχος προστασίας που απαγορεύει την πρόσβαση στο διαδίκτυο σε συσκευές SIGFox χωρίς να περνούν από τον πυρήνα δικτύου SIGFox, και τα δεδομένα προστατεύονται τόσο κατά την μεταφορά όσο και κατά την αποθήκευσή τους. Η ασφάλεια των δεδομένων κατά την μεταφορά επιτυγχάνεται μέσω ελέγχου ταυτότητας μηνυμάτων και αποφυγής αναπαραγωγής. Μέσω της χρήσης ενός τεκμηρίου μηνύματος και ενός κλειδιού αυθεντικοποίησης, η επαλήθευση του τεκμηρίου εξασφαλίζει την

αυθεντικοποίηση του αποστολέα και την ακεραιότητα του μηνύματος. Για την ασφάλεια των δεδομένων κατά την αποθήκευσή τους, οι βάσεις του SIGFox και το κύριο δίκτυο χρησιμοποιούν εμπιστευμένη πλατφόρμα μονάδας, γνωστή και ως ISO/IEC 11889, για την ασφάλεια του υλικού μέσω ενσωματωμένων κρυπτογραφικών κλειδιών.

Ασφάλεια μακροπρόθεσμης εξέλιξης (LTE): Το LTE είναι η κύρια τεχνολογία κινητής τηλεφωνίας 4G που χρησιμοποιείται παγκοσμίως σήμερα για την υποστήριξη κινητών τηλεπικοινωνιών. Όσον αφορά την ασφάλεια, ο Αμερικανικός Εθνικός Οργανισμός Επιστήμης και Τεχνολογίας (NIST) έχει δημοσιεύσει μια εκτενή έκθεση σχετικά με την ασφάλεια του LTE , η οποία περιλαμβάνει: (α) ασφάλεια υλικού, (β) κρυπτογραφία, (γ) ασφάλεια διεπαφής, (δ) ασφάλεια E-UTRAN, (ε) ασφάλεια ανάδρομης σύνδεσης και (δ) ασφάλεια πυρήνα δικτύου. Τα στοιχεία υποδομής του LTE (π.χ. εξελιγμένος κόμβος B, οντότητα διαχείρισης κινητικότητας, πύλη εξυπηρέτησης) μπορεί να χρησιμοποιούν εμπορικά υλικό, firmware και λογισμικό, καθιστώντας το

ευάλωτο σε γνωστές δημοσίως ελαττωματικές εφαρμογές λογισμικού. Οι απειλές που στοχεύουν στα δίκτυα LTE περιλαμβάνουν:

• Επιθέσεις κακόβουλου λογισμικού
• Ακρόαση των 2 πλευρών
• Παρεμπόδιση ραδιοκυμάτων
• Φυσικές επιθέσεις σε υποδομές

Η ασφάλεια των ενσύρματων δικτύων θα απαιτήσει επίσης την ασφάλεια του ενσύρματου συνδέσμου. Οι περισσότερες ενσύρματες συνδέσεις πραγματοποιούνται μέσω Ethernet, μέσω καλωδίων ή οπτικών ινών. Δεν υπάρχει τίποτα που να εμποδίζει κάποιον από το να ακουμπήσει έναν ενσύρματο σύνδεσμο για να εξετάσει τα εξελισσόμενα κύματα και να

προσπαθήσει να ανακτήσει δεδομένα, αλλά με κρυπτογραφημένα σήματα, η ανάκτηση είναι δύσκολη.

Ασφάλεια πρωτοκόλλου: Εκτός από την 'ασφάλεια σύνδεσης', υπάρχει επίσης ανάγκη για ασφάλεια που ενσωματώνεται στο πρωτόκολλο, δηλαδή 'ασφάλεια πρωτοκόλλου'. Η πλειοψηφία των δεδομένων στο διαδίκτυο μέσω ενσύρματων ή ασύρματων συνδέσεων χρησιμοποιούν το πρωτόκολλο ελέγχου μετάδοσης/πρωτόκολλο διαγράμματος χρήστη/συμπλέγματος πρωτοκόλλου Διαδικτύου (TCP/UDP/IP). Η πρόσβαση στο διαδίκτυο και η παροχή υπηρεσιών είναι καίρια για πολλούς οικιακούς και επαγγελματικούς χρήστες. Η διακοπή στην παροχή υπηρεσιών διαδικτύου μπορεί να προκαλέσει την αναστολή πολλών επιχειρηματικών λειτουργιών κ.λπ. Η εικόνα 12 παρουσιάζει μια λίστα από πρωτόκολλα με ενεργοποιημένη ασφάλεια για την παροχή ασφάλειας δικτύου και τερματικού σημείου.

Protocol security	Remarks
• IPSec	uses encapsulating security payload and authentication header to encrypt and authenticate data and tunnels (packet encapsulation) to form VPN
• DNSSec	protect against multiple concurrent requests for name resolution, thereby avoid overloading and crashing the server
• HTTPS	protection for web users in accessing data and web pages
• TLS	transport layer security (TLS) is a cryptographic protocol that provides end-to-end communications security over the Internet.
• SSL	secured socket layer (SSL) is used to provide a secured encrypted link for information transfer between a client and a web server.
• VPNs	provide a secured path for information transaction over the unknown route and over unsecured networks

Εικόνα 12 Λίστα πρωτοκόλλων ασφαλείας που ενσωματώνουν προστασία σε δίκτυα

4.3.4: Διασφάλιση δεδομένων

Οι περισσότερες εφαρμογές έξυπνων πόλεων θα αισθανθούν, θα συλλέξουν, θα επεξεργαστούν και θα αναλύσουν δεδομένα για να παράγουν σημαντικές ενδείξεις και να χρησιμοποιήσουν αυτές τις ενδείξεις για τη δημιουργία σημαντικών υπηρεσιών. Για παράδειγμα, οι εφαρμογές έξυπνης μεταφοράς θα συλλέγουν δεδομένα οχημάτων, οδηγών, κυκλοφοριακών ροών και επιβατών, ενώ οι εφαρμογές έξυπνης υγείας θα συλλέγουν δεδομένα ασθενών και γιατρών. Ανεξαρτήτως του ποιες είναι οι εφαρμογές έξυπνης πόλης, τα δεδομένα θα δημιουργούνται ως μέρος της πλατφόρμας έξυπνης πόλης και αυτά πρέπει να προστατευθούν, τόσο στο περιεχόμενο όσο και στην αποθήκευσή τους. Τέτοια δεδομένα μπορούν να προστατευθούν με διάφορους τρόπους:
(α) Έλεγχος πρόσβασης - αποκλεισμός μη εξουσιοδοτημένης πρόσβασης στα δεδομένα.
(β) Κρυπτογράφηση - προστασία του περιεχομένου των δεδομένων.
(γ) Ταυτοποίηση - επαλήθευση της πηγής.
(δ) Υπογραφές - επιβεβαίωση της εγκυρότητας των δεδομένων.
(ε) Απορρήτου - αποσυνδέουν τα δεδομένα από την ταυτότητα και την τοποθεσία του χρήστη.

Πρόσφατα, έχουν σημειωθεί περιστατικά παραβίασης δεδομένων, όπως η διαρροή προσωπικών δεδομένων από την Equifax , η απώλεια προσωπικών δεδομένων ηλεκτρονικού ταχυδρομείου από την Yahoo , η απώλεια δεδομένων πελατών από τη Citibank και την Standard Chartered . Όλα αυτά έχουν προκαλέσει δημόσια αντίδραση και έχουν κινητοποιήσει κλήσεις για δράση της κυβέρνησης. Επομένως, για μια έξυπνη πόλη, πρέπει να εξετάσουμε τον προστασία των διαφόρων τύπων δεδομένων που σχετίζονται με κάθε εφαρμογή έξυπνης πόλης και να καταστήσουμε το αντίστοιχο φορέα υπεύθυνο , όπως φαίνεται στις εικόνες 13 και 14. Από την εικόνα 13 φαίνεται πως, ένα μεγάλο μέρος των δεδομένων βρίσκεται υπό την ευθύνη της κυβέρνησης. Επομένως, οι

κυβερνήσεις θα πρέπει να εγκαθιδρύσουν ολοκληρωμένες πολιτικές και πλαίσια για την προστασία των δεδομένων. Για παράδειγμα, στις Ηνωμένες Πολιτείες, το Υπουργείο Εμπορίου και το δικαστικό σύστημα έχουν επιβάλει πρόστιμο στην Yahoo Inc. για τη διαρροή δεδομένων. Οι φορείς από ιδιωτικά ιδρύματα πρέπει επίσης να εξασφαλίζουν ότι οι μέθοδοί τους για την προστασία των δεδομένων των πελατών πραγματικά πληρούν αυστηρές απαιτήσεις.

Οι κανονισμοί, τα πρότυπα και οι βέλτιστες πρακτικές για την προστασία των δεδομένων εξελίσσονται. Ακόμα και μέχρι σήμερα δεν έχει εμφανιστεί κάποιο παγκόσμιο πρότυπο. Στην Ευρωπαϊκή Ένωση (ΕΕ), ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 ('GDPR') εισάχθηκε, καλύπτοντας την προστασία δεδομένων και την Ιδιωτικότητα για όλα τα άτομα εντός της ΕΕ και της Ευρωπαϊκής Οικονομικής Περιοχής (ΕΟΠ). Αφορά επίσης την εξαγωγή προσωπικών δεδομένων έξω από την ΕΕ και την ΕΟΠ.

Η Οδηγία της Ευρωπαϊκής Επιτροπής για την Προστασία Δεδομένων εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο και τους υπουργούς από τις εθνικές κυβερνήσεις το 1995. Η οδηγία περιλαμβάνει βασικές αρχές που πρέπει να συμμορφώνονται τα κράτη μέλη. Στην επεξεργασία προσωπικών δεδομένων, πρέπει να συμμορφώνεστε με οκτώ επιβεβλημένες αρχές καλών πρακτικών.

Αυτές είναι:

(α) Δίκαιη και νόμιμη επεξεργασία

(β) Επεξεργασία για περιορισμένους σκοπούς

(γ) Επαρκής, σχετική και όχι υπερβολική

(δ) Ακριβής

(ε) Διατηρούμενη όσο απαιτείται

(στ) Επεξεργασία σύμφωνα με τα δικαιώματα του υποκειμένου δεδομένων

(η) Ασφαλής

(θ) Μεταφορά μόνο σε χώρες με επαρκή προστασία.

Στις Ηνωμένες Πολιτείες, οι νόμοι εισάγονται για να διασφαλίζουν τη χρήση μέτρων ασφαλείας πληροφοριών. Κάποιες από τις πρόσφατες ενέργειες που εισήχθησαν περιλαμβάνουν:

• Νόμος του 2000 του Κογκρέσου των ΗΠΑ για Ψηφιακές Υπογραφές στον Παγκόσμιο Εθνικό Εμπόριο.

• Νόμος Εθνικής Ασφάλειας του 2002.

• Ο Νόμος του 2002 για τη Διαχείριση της Πληροφορικής και της Ασφάλειας της Πληροφορίας του 2014.

Επομένως, η χρήση τεχνολογιών από μόνη της δεν μπορεί να προστατεύσει πλήρως και επαρκώς τα δεδομένα. Χρειάζονται νόμοι και κανονισμοί για να διασφαλιστεί η συμμόρφωση από τις οργανώσεις που κατέχουν και είναι υπεύθυνες για την επεξεργασία δεδομένων.

Types of data to secure		Remarks
transport	•	aviation travel records
	•	land transport data
	•	driver data
	•	vehicle data
	•	trains, buses, taxis, etc.
	•	traffic lights
health	•	patient records
	•	doctor records
	•	medical supplies records
	•	medical staffs' information
finance	•	personal financial data
	•	business financial data
	•	tax data
utility	•	water usage
	•	electricity usage
	•	gas usage
	•	users (consumers) data
telecom	•	subscribers' data
	•	infrastructure data
	•	utilisation data
	•	transactions data

Εικόνα 13 Λίστα δεδομένων προς ασφάλιση σε μια έξυπνη πόλη

Types of data	Responsible entity
• citizens' data	• government
• financial data	• financial institutions
• urban data	• government
• utilities data	• providers and government
• transport data	• government
• health data	• healthcare providers and government
• weather data	• government
• criminal data	• law-enforcers and government
• housing data	• government

Εικόνα 14 Λίστα κρίσιμων δεδομένων που πρέπει να προστατεύονται και οι υπεύθυνοι φορείς σε μια έξυπνη πόλη

4.3.5: Διασφάλιση των οικονομικών περιουσιακών στοιχείων της έξυπνης πόλης

Οι χρηματοοικονομικοί πόροι περιλαμβάνουν τόσο υλικά όσο και άυλα αγαθά από τους κατοίκους της πόλης, επιχειρηματικές εταιρείες και την κυβέρνηση. Το μεγαλύτερο μέρος αυτών των χρηματοοικονομικών πόρων κατέχεται από χρηματοπιστωτικά ιδρύματα, είτε πρόκειται για τράπεζες, εταιρείες ασφάλειας ή συνεταιριστικά ιδρύματα. Πιθανές επιθέσεις περιλαμβάνουν:

- απενεργοποίηση χρηματοοικονομικών υπηρεσιών (όπως online τραπεζικές υπηρεσίες, online συναλλαγές κλπ.)
- κλοπή χρημάτων (κλοπή χρημάτων, μετοχών κλπ.)
- κλοπή πληροφοριών λογαριασμών (χρήστη και χρηματοοικονομικά δεδομένα)

Τα διάφορα μέτρα προστασίας (π.χ. firewalls) χρησιμοποιούνται κυρίως για την προστασία των χρηματοοικονομικών συστημάτων πληροφορικής από τους επιτιθέμενους, μαζί με συστήματα ανίχνευσης και πρόληψης παραβάσεων. Η ασφάλεια σε όρους ελέγχου πρόσβασης χρηστών,

ταυτοποίησης χρηστών, κρυπτογράφησης δεδομένων, ασφαλούς δικτύου και μεταφοράς συνδέσεων, προστασίας από κακόβουλο λογισμικό και ιούς, έλεγχος καταγραφής καταγραφών, προστασία άκρων κλπ., είναι όλα απαραίτητα για την προστασία των χρηματοοικονομικών πόρων μιας έξυπνης πόλης.

4.3.6: Διασφάλιση των κρίσιμων υπηρεσιών έξυπνης πόλης

Στην περίπτωση που οι υπηρεσίες της πόλης (όπως η παροχή ηλεκτρικού ρεύματος, αερίου κλπ.) διακόπτονται από επιτιθέμενους, η ζωή εκατομμυρίων κατοίκων της πόλης θα είναι γεμάτη προβλήματα. Αυτό είναι ένα μείζον καταστροφικό γεγονός. Η εικόνα 15 δείχνει μια λίστα πιθανών επιθέσεων και τις επιπτώσεις λόγω της διακοπής αρκετών τύπων κρίσιμων υπηρεσιών.

Η διακοπή της επιβολής του νόμου (αστυνομίας) και των επιχειρήσεων διάσωσης από πυρκαγιές είναι επίσης θανατηφόρα. Επιπλέον, η διακοπή των υπηρεσιών μεταφοράς (τρένων, λεωφορείων, ταξί, πτήσεων) και των φαναριών κυκλοφορίας είναι επίσης καταστροφική (η κακή χρήση των φαναριών κυκλοφορίας μπορεί να οδηγήσει σε ατυχήματα και κυκλοφοριακή συμφόρηση). Η διακοπή των βασικών υπηρεσιών της πόλης θεωρείται έγκλημα και πράξη τρομοκρατίας σε πολλές χώρες σήμερα. Μια έξυπνη πόλη πρέπει, συνεπώς, να ασφαλίζει όλες τις βασικές της υπηρεσίες. Οι επιθέσεις στις κρίσιμες υπηρεσίες μιας έξυπνης πόλης μπορεί να λάβουν τη μορφή:

(α) Αρνητικής υπηρεσίας - τελική διακοπή της παροχής των βασικών υπηρεσιών της πόλης.

(β) Διακοπή των υπηρεσιών - διακοπές της διαθεσιμότητας των υπηρεσιών της πόλης.

Type of critical services	Remarks
water	• disrupt the supply of water to households and businesses • resulting in public outcry and threatening personal health
gas	• hinder the delivery of gas to households • leaving residents unable to cook food
electricity	• disrupt the supply of electricity to the city • resulting in city blackouts and an unsafe environment
police	• hinder and delay the summon of police • resulting in crimes unattended to and loss of lives
fire rescue	• hinder and delay the summon of fire rescue • resulting in property damage and lives lost
traffic lights	• create traffic disorientation, jams, delays, and accidents • create chaos on the streets • hinder the delivery of services
public lifts	• maliciously disrupt the normal operation of lifts • causing delays, accidents, and anxiety
waste clearance	• household rubbish clearance services are disrupted • threatening public hygiene, health, and safety of residents
public environmental cleaning	• falsify video images of street cleanliness • resulting in dirty and unhygienic streets, drains, and parks
public parking services	• blockage of parking by falsifying status of no parking spaces • resulting in road congestion and anxiety
payment of utility bills	• payment of bills prevented or not registered • resulting in unexpected termination of utility services
banking services	• withdrawal of money prevented • credit card transaction services halted • financial transactions interrupted or financial theft
aviation services	• disrupt travel services at airport • passengers strangled at airports, creating chaos and distress

Εικόνα 15 Τύποι υπηρεσιών έξυπνης πόλης και πιθανές επιθέσεις

4.4 Συστήματα Ασφαλείας στις Έξυπνες Πόλεις

4.4.1: Οι καλύτερες πρακτικές για ασφάλεια στις έξυπνες πόλεις

Σύμφωνα με το Ευρωπαϊκό Ινστιτούτο Δικτύων και Πληροφοριών, έχει εντοπιστεί μια λίστα με τις καλύτερες πρακτικές για την κυβερνοασφάλεια των έξυπνων πόλεων. Αυτές είναι:

• Χρήση VPNs
• Κρυπτογράφηση δεδομένων
• Χρήση συστημάτων ανίχνευσης διείσδυσης στο δίκτυο
• Χρήση φυσικής προστασίας
• Εγκατάσταση ελέγχου πρόσβασης
• Εγκατάσταση συναγερμών και παρακολούθησης
• Εφαρμογή πολιτικής ασφάλειας
• Δημιουργία αρχείων δραστηριότητας
• Διατήρηση αντιγράφων ασφαλείας
• Τακτικός έλεγχος

Η εισαγωγή των βέλτιστων πρακτικών είναι μια καλή προσέγγιση για πολλές χώρες ώστε να υλοποιούν και να μαθαίνουν από τις εμπειρίες των άλλων. Κάθε έξυπνη πόλη θα πρέπει να συμβάλλει στον καθορισμό των βέλτιστων πρακτικών ασφάλειας, να αναφέρει και να μοιράζεται κάθε ευπάθεια, έτσι ώστε τέτοια περιστατικά να μην επαναλαμβάνονται σε άλλες πόλεις. Εκτός από τις προσπάθειες που καταβάλλει ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύου και Πληροφοριών (ENISA), το αμερικανικό Εθνικό Ινστιτούτο Πρότυπων και Τεχνολογίας (NIST) , αντιμετωπίζει αυτά τα θέματα με την εισαγωγή ενός πλαισίου κυβερνοασφάλειας, όπως φαίνεται στην εικόνα. Ο κύριος σκοπός του πλαισίου είναι να αναπτύξει ένα κοινό γλωσσικό όρο για καλύτερη κατανόηση και ερμηνεία των κινδύνων από τους εμπλεκόμενους φορείς.

Το πλαίσιο παρουσιάζει πέντε κύριες λειτουργίες όπως:

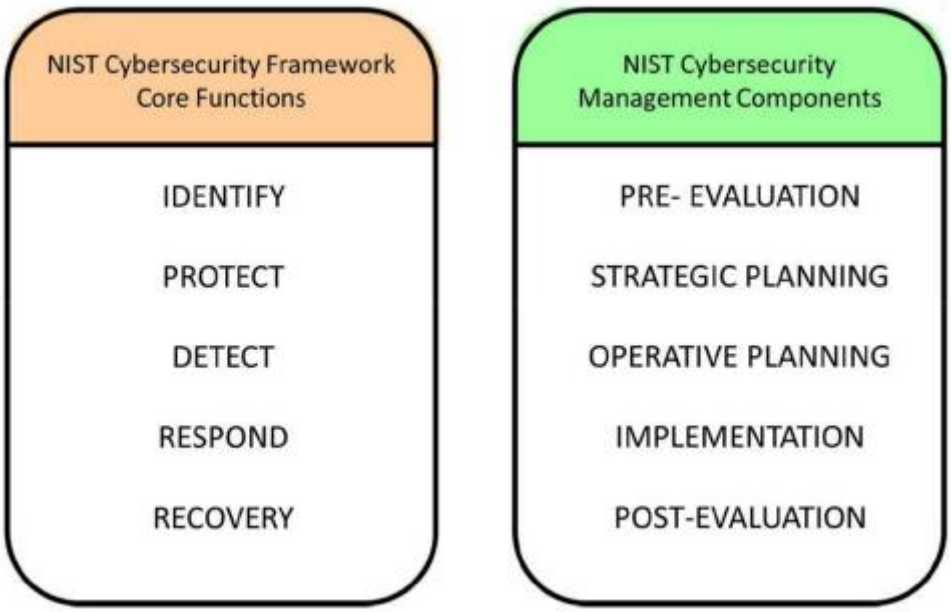
(a) **Αναγνώριση** - για να αναπτύξει μια κατανόηση των κινδύνων που σχετίζονται με ανθρώπους, συστήματα, περιουσίες, δεδομένα και ικανότητες.

(b) **Προστασία** - για να αναπτύξει μέτρα προστασίας για τον περιορισμό και την περιορισμένη διαχείριση ενός συμβάντος ασφάλειας, προστατεύοντας και εξασφαλίζοντας την παροχή υπηρεσιών.

(c) **Ανίχνευση** - για να αναπτύξει μεθόδους για τον εντοπισμό παραβιάσεων ασφάλειας και ανωμαλιών.

(d) **Αντίδραση** - για να αντιδράσει σε ένα συμβάν περιορίζοντάς το, περιορίζοντας τη βλαβερή του επίδραση.

(e) **Ανάκτηση** - για την άμεση αποκατάσταση των ικανοτήτων και των υπηρεσιών που πλήττονται από το συμβάν ασφάλειας και την πρόληψη περαιτέρω παρόμοιων επιθέσεων.



Εικόνα 16 Βασικές λειτουργίες και διαχείριση του πλαισίου κυβερνοασφάλειας NIST

4.4.2: Αναγνώριση κλώνων προσώπου σε περίπτωση απάτης

Με την αυξανόμενη εξάρτηση από το βίντεο και την αναγνώριση προσώπου στις έξυπνες πόλεις, πολλά συστήματα δημόσιας ασφάλειας χρησιμοποιούν τεχνολογίες τεχνητής νοημοσύνης και αναγνώρισης προσώπου για την ταυτοποίηση επιζητούμενων εγκληματιών ή αγνοουμένων προσώπων. Επιπλέον, πολλά συστήματα εισόδου σε καταστήματα, επιχειρήσεις και ελέγχου διαβατηρίων σε ολόκληρο τον κόσμο έχουν αρχίσει να χρησιμοποιούν τεχνολογία αναγνώρισης προσώπου για το σκανάρισμα και την επικύρωση ταξιδιωτών, επισκεπτών, αγοραστών και εξουσιοδοτημένου προσωπικού. Η αυξανόμενη εξάρτηση μπορεί να έχει αρνητικές επιπτώσεις, καθώς οι εγκληματίες/επιτιθέμενοι μπορούν να υποκριθούν άλλους για να κρύψουν την ταυτότητά τους κατά τη διάρκεια εγκληματικών ενεργειών σε δημόσιους ή ιδιωτικούς χώρους. Πράγματι, υπάρχουν ήδη αρκετές περιπτώσεις όπου η απάτη με τη χρήση μάσκας από σιλικόνη (βλ. εικόνα. 17) έχει οδηγήσει σε εκατομμύρια οικονομικές απώλειες (βλ. εικόνα 16). Ένα σημαντικό κομμάτι της ασφάλειας για τις μελλοντικές έξυπνες πόλεις είναι να επιβεβαιώνεται η ταυτότητα των ατόμων πέρα από την απλή αναγνώριση προσώπου, χρησιμοποιώντας βιομετρικά δεδομένα, αναγνώριση ίριδας, αποτυπώματα δακτύλων, φωνή, γραφή κλπ. Αυτό ανοίγει τον δρόμο για περαιτέρω έρευνα.

Εικόνα 17 Η τεχνολογία μάσκας σιλικόνης σήμερα μπορεί να δημιουργήσει πρόσωπα που μοιάζουν με ανθρώπους που δυνητικά μπορούν να μιμηθούν οποιονδήποτε και να ξεγελάσει την αναγνώριση προσώπου

Κεφάλαιο 5: Η ιδιωτικότητα στις Smart Cities

Η ιδιωτικότητα πρέπει να θεωρείται ως σημαντικός παράγοντας κατά τον σχεδιασμό και την υλοποίηση έξυπνων λύσεων σε πόλεις. Η ισορροπία μεταξύ των οφελών της τεχνολογίας και της προστασίας της ιδιωτικότητας πρέπει να διατηρείται, προκειμένου να διασφαλιστεί ότι οι Έξυπνες Πόλεις εξυπηρετούν το κοινό συμφέρον χωρίς να θίγουν την προσωπική ιδιωτικότητα των πολιτών.

Για το επιχειρηματικό του σχέδιο και την επίδρασή του, ο ψηφιακός πολιτισμός πρέπει να τροφοδοτείται με μεγάλα δεδομένα: Χωρίς μεγάλα δεδομένα, το λογισμικό είναι «ανήμπορο» και ανόητο. Πώς μπορούμε να συμβιβάσουμε την ιδιωτικότητα σε μια αστική κοινωνία όπου κάθε πολίτης θα βρίσκεται υπό παρακολούθηση σε δημόσιους χώρους , ακόμα και στο σπίτι του; Η παρακολούθηση , λαμβάνει χώρα λόγω της ανάγκης να βελτιωθεί η πόλη, για να αναλύσει τη ροή κίνησης, τη χρήση των δημόσιων χώρων, την κατανάλωση ενέργειας, τα επίπεδα απορριμμάτων.

Πόσο πρέπει να προχωρήσουμε στην παρακολούθηση και τον σχεδιασμό του προφίλ καθημερινής συμπεριφοράς κάθε πολίτη; Ποιος μπορεί να συλλέξει, να αποθηκεύσει, να μοιραστεί ή να πουλήσει, να επεξεργαστεί και να χρησιμοποιήσει αυτά τα δεδομένα; Σε ποιους όρους "Συμφωνίας Δεδομένων" αναγράφονται τα παραπάνω;

Αντιμετωπίζοντας αυτές τις προκλήσεις, οι εθνικοί νομοθετικοί κανονισμοί και η επαγγελματική ηθική του 20ου αιώνα είναι ξεπερασμένοι ή αναποτελεσματικοί για να αντιμετωπίσουν ένα νέο φαινόμενο που είναι χαρακτηριστικό της αναδυόμενης ψηφιακής πολιτισμικής και των φιλοδοξιών των παγκοσμίων ψηφιακών εταιρειών. Μια νέα κοινωνική συμφωνία (Η λεγόμενη ‘Συμφωνία Δεδομένων’) είναι τώρα απαραίτητη και οι έξυπνες πόλεις που παραβλέπουν αυτήν την πτυχή βρίσκονται σε κίνδυνο.

5.1: Προστασία των προσωπικών δεδομένων στις smart cities

5.1.1: Τι είναι τα δεδομένα προσωπικού χαρακτήρα;

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα.
Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου, παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ (Γενικός Κανονισμός Προστασίας Δεδομένων).

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα με τέτοιον τρόπο ώστε το άτομο να μην είναι πια ταυτοποιήσιμο δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη.

Ο ΓΚΠΔ (Γενικός Κανονισμός Προστασίας Δεδομένων) προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βίντεο επιτήρησης ή σε έντυπη μορφή. Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει ο ΓΚΠΔ (Γενικός Κανονισμός Προστασίας Δεδομένων).

5.1.2: Παραδείγματα δεδομένων προσωπικού χαρακτήρα

Οι προσωπικές πληροφορίες αποτελούν ένα ανεκτίμητο μέρος της ψηφιακής μας ταυτότητας και επικοινωνίας. Ανάμεσά τους περιλαμβάνονται:

1. Όνομα και επώνυμο
2. Διεύθυνση κατοικίας
3. Ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com·
4. Αναγνωριστικός αριθμός κάρτας
5. Δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
6. Διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
7. Αναγνωριστικό cookie
8. Το αναγνωριστικό διαφήμισης του τηλεφώνου σας
9. Δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

Αυτά τα δεδομένα μπορούν να παρέχουν σημαντικές πληροφορίες για την ταυτότητα, τις προτιμήσεις και την καθημερινή ζωή ενός ατόμου.

5.2 : Προκλήσεις για την Ιδιωτικότητα στις Έξυπνες Πόλεις

Οι κίνδυνοι της υποδομής μιας έξυπνης πόλης παρουσιάζονται σε τρεις κατηγορίες: απειλές, ευπάθειες και συνέπειες. Επειδή οι κυβερνοχώροι και οι υποδομές αυτών είναι ενσωματωμένοι στις έξυπνες πόλεις, οποιαδήποτε επιτυχημένη επίθεση σε αυτούς μπορεί να οδηγήσει σε απτά αποτελέσματα στον πραγματικό κόσμο, επιδεινώνοντας έτσι την παράμετρο του αποτελέσματος. Η ευπάθεια αυτών των πόλεων αυξάνεται με την αύξηση του επιπέδου επιθέσεων. Γενικά, στην έξυπνη πόλη, λόγω του χαρακτηριστικού της κατανόησης του περιβάλλοντος και της ικανότητας παρακολούθησης και ελέγχου των συμπεριφορών και ενεργειών των χρηστών/πολιτών αυτής, η Ιδιωτικότητα βρίσκεται σε σοβαρό κίνδυνο, κάτι που μπορεί να αποτελέσει

σοβαρό κίνδυνο για τις ζωές των ανθρώπων. Αυτή η παράγραφος θα συζητήσει τις πιο κρίσιμες απειλές για την ιδιωτικότητα στις έξυπνες πόλεις.

5.2.1: Ζητήματα προστασίας προσωπικών δεδομένων

Η προστασία δεδομένων εντός του πλαισίου των έξυπνων πόλεων μπορεί να αντιληφθεί από διάφορες οπτικές γωνίες. Πρώτα απ' όλα, πρέπει να ληφθεί υπόψη ότι όταν εξετάζουμε τις έξυπνες πόλεις υπάρχουν διαφορετικοί νομοθετικοί κανονισμοί σε πολλά μέρη του κόσμου και επομένως η ρύθμισή τους δεν είναι ομοιόμορφη. Εάν λάβουμε υπόψη την ευρωπαϊκή κατάσταση, ξεκινώντας από μια εστιασμένη , στον χρήστη-πολίτη, προοπτική και λαμβάνοντας υπόψη τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), μπορούμε να εξάγουμε σημαντικές αρχές με μεγάλη σημασία για τις έξυπνες πόλεις. Ο GDPR ενσωματώνει ένα σύνολο βασικών αρχών και κανόνων που πρέπει πάντοτε να λαμβάνονται υπόψη στο πλαίσιο των έξυπνων πόλεων. Μεταξύ αυτών: νομιμότητα, δικαιοσύνη, διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια, περιορισμός αποθήκευσης, ακεραιότητα και ευθύνη. Ο GDPR παρέχει επίσης λεπτομερείς κανόνες για τη συλλογή συγκατάθεσης. Ο GDPR είναι πιο προστατευτικός όσον αφορά τις προϋποθέσεις για τη συγκατάθεση, ωστόσο οι νέοι κανόνες μεταφράζουν σε νόμο αυτό που ζητείτο ήδη από ορισμένες εποπτικές αρχές. Σύμφωνα με το άρθρο 4(11) του GDPR, η συγκατάθεση σημαίνει "κάθε ελεύθερα δοθείσα, συγκεκριμένη, ενημερωμένη και αμφίβολη ένδειξη των επιθυμιών του υποκειμένου δεδομένων με την οποία αυτός ή αυτή, με δήλωση ή με σαφή θετική ενέργεια, δηλώνει συμφωνία για την επεξεργασία προσωπικών δεδομένων που τον ή την αφορούν". Ο GDPR επίσης κάνει ακριβή την απαίτηση για την επεξεργασία προσωπικών δεδομένων ανηλίκων και την επεξεργασία ειδικών κατηγοριών δεδομένων. Ο GDPR ορίζει υποχρεώσεις προς τη διευκόλυνση της άσκησης του δικαιώματος του υποκειμένου δεδομένων σε πληροφόρηση, όπως η πρόσβαση στα προσωπικά δεδομένα, η διόρθωση και η διαγραφή, το δικαίωμα στη φορητότητα των δεδομένων. Οι νομικές διατάξεις επίσης επιτρέπουν στο

υποκείμενο των δεδομένων να περιορίσει την επεξεργασία των δεδομένων του υπό ορισμένες περιστάσεις και λεπτομερείς διαδικασίες για την προστασία του ατόμου απέναντι σε μηχανισμούς αυτοματοποιημένων αποφάσεων.

5.2.2: Ζητήματα σχετικά με την ταυτοποίηση των χρηστών

Η ταυτοποίηση αναφέρεται στη διαδικασία σύνδεσης ενός αναγνωριστικού στοιχείου, όπως το όνομα ή η διεύθυνση ενός ατόμου, με ιδιωτικά δεδομένα που αφορούν αυτό το άτομο. Αυτή η διαδικασία μπορεί να οδηγήσει σε σημαντικές απειλές για την ιδιωτικότητα, καθώς προσωπικά δεδομένα μπορεί να αποκαλυφθούν και να χρησιμοποιηθούν χωρίς την έγκριση ή τη γνώση του ατόμου.
Δηλαδή , η απειλή ταυτοποίησης είναι η σύνδεση ενός αναγνωριστικού (π.χ., όνομα, διεύθυνση) με ιδιωτικά δεδομένα σχετικά με ένα άτομο. Το Διαδίκτυο των Πραγμάτων (Internet of Things, IoT) είναι ένα δίκτυο συνδεδεμένων συσκευών που επικοινωνούν μεταξύ τους και ανταλλάσσουν δεδομένα μέσω του διαδικτύου. Καθώς αυξάνεται ο αριθμός αυτών των συνδεδεμένων συσκευών, αυξάνεται και η ποσότητα των δεδομένων που συλλέγονται και ανταλλάσσονται, γεγονός που ενισχύει την απειλή της ταυτοποίησης. Οι συσκευές αυτές μπορούν να συλλέγουν ποικίλα δεδομένα, όπως προσωπικές συνήθειες, τοποθεσίες, και άλλες ευαίσθητες πληροφορίες.

5.2.3: Ζητήματα σχετικά με τον εντοπισμό και την παρακολούθηση τοποθεσίας των χρηστών

Ο εντοπισμός και η παρακολούθηση αποτελούν σοβαρή απειλή για την ιδιωτικότητα των ατόμων, καθώς η δυνατότητα εντοπισμού της τοποθεσίας ενός ατόμου και η καταγραφή των κινήσεών του μπορούν να χρησιμοποιηθούν για την παραβίαση των προσωπικών του δεδομένων. Η αύξηση της διαθεσιμότητας χωρικών δεδομένων, όπως γεωγραφικές πληροφορίες από smartphones και άλλες έξυπνες συσκευές, έχει οδηγήσει σε μια αυξανόμενη ενασχόληση με την ανάλυση αυτών των δεδομένων. Το Διαδίκτυο των Πραγμάτων (IoT) προσθέτει μια νέα

διάσταση σε αυτή την πρόκληση, καθώς οι συσκευές IoT, που περιλαμβάνουν αισθητήρες, κάμερες, και άλλες τεχνολογίες, καταγράφουν συνεχώς δεδομένα σχετικά με την ταυτότητα, την τοποθεσία και τις δραστηριότητες των χρηστών τους.
Αυτή η συνεχής καταγραφή μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, από την παροχή εξατομικευμένων υπηρεσιών και διαφημίσεων, μέχρι την επιτήρηση και την επιβολή του νόμου.
Ωστόσο, εγείρει σοβαρά ζητήματα σχετικά με την ιδιωτικότητα και την ασφάλεια των προσωπικών δεδομένων. Η ανεξέλεγκτη συλλογή και ανάλυση χωρικών δεδομένων μπορεί να οδηγήσει σε κατάχρηση της πληροφορίας, παραβιάζοντας την ιδιωτική ζωή των ατόμων και ενδεχομένως θέτοντάς τους σε κίνδυνο.

5.2.4: Ζητήματα σχετικά με τα σφάλματα λογισμικού στις έξυπνες πόλεις

Ένα απλό σφάλμα λογισμικού μπορεί να επηρεάσει σημαντικά το σύστημα, δεδομένου ότι οι έξυπνες πόλεις περιέχουν τόσα πολλά συστήματα και συσκευές. Τα σφάλματα λογισμικού είναι αναπόφευκτα στο πλαίσιο της ανάπτυξης και της λειτουργίας των τεχνολογικών συστημάτων. Σε μια έξυπνη πόλη, όπου η τεχνολογία είναι συνυφασμένη με την καθημερινή λειτουργία και διαχείριση των υποδομών, η ύπαρξη σφαλμάτων μπορεί να έχει σοβαρές συνέπειες. Ένα απλό σφάλμα λογισμικού μπορεί να προκαλέσει δυσλειτουργίες σε ζωτικής σημασίας συστήματα, όπως η κυκλοφοριακή διαχείριση, η παροχή ενέργειας ή οι επικοινωνίες. Λόγω της διασύνδεσης και της αλληλεξάρτησης των διαφόρων συσκευών και συστημάτων σε μια έξυπνη πόλη, οι επιπτώσεις ενός σφάλματος μπορεί να εξαπλωθούν γρήγορα και να προκαλέσουν ευρύτερα προβλήματα. Είναι επομένως κρίσιμο να υπάρχει συνεχής παρακολούθηση, δοκιμή και συντήρηση των λογισμικών για να ελαχιστοποιούνται οι κίνδυνοι και να διασφαλίζεται η ομαλή λειτουργία των έξυπνων πόλεων.

5.2.5: Ζητήματα σχετικά με τις κλασικές απειλές στο διαδίκτυο των πραγμάτων (IoT)

Υπάρχουν από την αρχή του Διαδικτύου και εξακολουθούν να χρησιμοποιούνται σε δίκτυα βασισμένα σε IoT επειδή ένα μεγάλο μέρος των πληροφοριών του δικτύου μεταδίδεται μέσω του Διαδικτύου.

1. **Κακόβουλο Λογισμικό (Malware):** Το κακόβουλο λογισμικό αποτελεί μια από τις κύριες απειλές για τα δίκτυα IoT. Μπορεί να εγκατασταθεί σε συσκευές IoT μέσω ευπαθειών στο λογισμικό ή μέσω ανεπιθύμητων παρεμβάσεων. Αυτό μπορεί να οδηγήσει στην παράνομη πρόσβαση, την κλοπή δεδομένων ή ακόμη και τον έλεγχο των συσκευών από εξωτερικούς εισβολείς.
2. **Επιθέσεις Phishing:** Οι επιθέσεις phishing αποσκοπούν στην απόκτηση ευαίσθητων πληροφοριών, όπως κωδικοί πρόσβασης και προσωπικά δεδομένα, με ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου ή άλλες μορφές επικοινωνίας. Στο πλαίσιο του IoT, αυτές οι επιθέσεις μπορούν να επικεντρωθούν σε διαδικτυακές συσκευές που είναι συνδεδεμένες στο δίκτυο, προκαλώντας πιθανά προβλήματα ασφαλείας.
3. **Ανεπιθύμητα Μηνύματα (Spam):** Το spam αναφέρεται σε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα κειμένου που στέλνονται μαζικά σε μεγάλους αριθμούς αποδεκτών. Ενώ στο παρελθόν το spam ήταν κυρίως μια ενόχληση, σήμερα μπορεί να περιλαμβάνει και κακόβουλους συνδέσμους ή αρχεία που μπορούν να μολύνουν συσκευές IoT με κακόβουλο λογισμικό και έτσι να κλαπούν προσωπικά δεδομένα.

5.2.6: Ζητήματα σχετικά με τις σύγχρονες απειλές στο διαδίκτυο των πραγμάτων (IoT)

Όταν αναφερόμαστε σε σύγχρονες απειλές εννοούμε στόχους προσωπικών πληροφοριών, διαρροές προσωπικών δεδομένων και χωρικών δεδομένων, ψεύτικα προφίλ, επιθέσεις προσομοίωσης ταυτότητας, αναγνώριση προσώπου, και επιθέσεις αναστολής είναι παραδείγματα αυτού του τύπου.

Για να το αναπτύξουμε λίγο περισσότερο, αυτοί οι τύποι απειλών αναφέρονται σε κίνδυνους που σχετίζονται με την προσωπική

ιδιωτικότητα και την ασφάλεια δεδομένων στον ψηφιακό κόσμο. Οι επιθέσεις μπορεί να περιλαμβάνουν την παραβίαση ατομικών λογαριασμών, τη διαρροή ευαίσθητων πληροφοριών, τη δημιουργία ψεύτικων προφίλ για απάτες ή ακόμα και τη χρήση της τεχνολογίας αναγνώρισης προσώπου για παραβίαση της ιδιωτικότητας. Αυτοί οι κίνδυνοι επιδιώκουν συχνά την κλοπή ατομικών δεδομένων ή ακόμα και την παραβίαση της ατομικής ταυτότητας για επιδιώξεις απάτης ή κακόβουλων δραστηριοτήτων.

5.3: Η ιδιωτικότητα από τον σχεδιασμό της έξυπνης πόλης (Privacy by design)

Η ιδιωτικότητα από τον σχεδιασμό συχνά αναφέρεται ως η στρατηγική για την επίλυση προβλημάτων ιδιωτικότητας στις έξυπνες πόλεις. Με αυτόν τον τρόπο, μπορεί να εξασφαλιστεί ότι η προστασία της ιδιωτικότητας λαμβάνεται υπόψη πριν, κατά τη διάρκεια και μετά τον σχεδιασμό οποιασδήποτε έξυπνης πόλης. Η ιδιωτικότητα από τον σχεδιασμό περιλαμβάνει επτά αρχές που πρέπει να τηρούνται.

Αυτές περιλαμβάνουν τα εξής:

1. Ενεργή προστασία της ιδιωτικότητας αντί για επαναληπτικές ενέργειες μετά από παραβίαση της ιδιωτικότητας.
2. Προεπιλεγμένες ρυθμίσεις ιδιωτικότητας
3. Η ιδιωτικότητα ενσωματώνεται στο σχεδιασμό
4. Πλήρεις λειτουργίες με πλήρη προστασία της ιδιωτικότητας
5. Προστασία της ιδιωτικότητας καθ' όλη τη διάρκεια του κύκλου ζωής των δεδομένων
6. Διαφάνεια
7. Σεβασμός της ιδιωτικότητας των χρηστών.

5.4: Αρχιτεκτονική της ιδιωτικότητας (Privacy Architecture)

Η αρχιτεκτονική ιδιωτικότητας αναφέρεται στον τρόπο με τον οποίο σχεδιάζονται και οργανώνονται τα συστήματα και οι εφαρμογές ώστε να διασφαλίζεται η προστασία των προσωπικών δεδομένων και η αποφυγή πιθανών διαρροών ιδιωτικότητας. Μια αρχιτεκτονική παράδοση περιγράφει τις βασικές συνιστώσες του συστήματος, τα καθήκοντά τους και τις σχέσεις μεταξύ τους. Επιπλέον, χρησιμοποιείται για να διαμορφώσει τα στοιχεία αυτά και τις σχέσεις τους με πιο λεπτομερή τρόπο. Συχνά, η έλλειψη υπαρκτών προτύπων για την προστασία της ιδιωτικότητας οδηγεί στην ανάγκη ανάπτυξης προσαρμοσμένων αρχιτεκτονικών για κάθε συγκεκριμένη περίπτωση.

5.5: Έλεγχος και λογοδοσία

Η επιθεώρηση από την πλευρά των πολιτών και η ευθύνη από την έξυπνη πόλη και τους παρόχους της υπηρεσίας πρέπει να εξετάζονται προσεκτικά, διεξοδικά και να λαμβάνονται υπόψη κατά τον σχεδιασμό του απορρήτου. Η ευθύνη στις έξυπνες πόλεις έχει δύο διαφορετικές σημασίες:

1. Να κρατά η πόλη υπεύθυνη για τη χρήση των δεδομένων των πολιτών και την τήρηση του απορρήτου των δεδομένων αυτών.

2. Να κρατά τους πολίτες υπεύθυνους και να τους καλεί για εξηγήσεις όταν λαμβάνει χώρα κάποια κακή συμπεριφορά.

Οι ανεξάρτητοι έλεγχοι επιτρέπουν στους ανθρώπους να κατανοήσουν πόσο συχνά συμβαίνει μια επίθεση στο απόρρητο, εάν χρησιμοποιούνται για τον δηλωμένο σκοπό τους και πόσο καλά επιτυγχάνουν αυτόν τον στόχο.

5.6 Νομοθετικό Πλαίσιο και Κανονιστικά Θέματα

5.6.1 GDPR και Άλλες Νομοθετικές Διατάξεις

Το GDPR θα απαιτήσει από τις έξυπνες πόλεις:

1. Τη χρήση του σχεδιασμού απόρρητου με βάση την προστασία των δεδομένων, την προεπιλογή του απορρήτου και τη χρήση της Αξιολόγησης Επιπτώσεων στην Προστασία των Δεδομένων κατά τον σχεδιασμό και τη διαχείριση των λύσεων πληροφορικής και επικοινωνιών (ICT – Information and Communication Technology) που χρησιμοποιούν προσωπικά δεδομένα.
2. Την οριοθέτηση προστασίας δεδομένων

Έχουμε βασικές αρχές για την εφαρμογή μέτρων απόρρητου με βάση τον σχεδιασμό μέσα στις έξυπνες πόλεις. Εδώ έχουμε διαφορετικές επιλογές:

- Οι επτά αρχές της Ann Cavoukian: ενεργητικότητα αντί αντίδρασης, απόρρητο ως προεπιλογή, απόρρητο με βάση τον σχεδιασμό, θετικό άθροισμα, ασφάλεια, διαφάνεια, επικεντρωμένο στον χρήστη. (Η Ann Cavoukian είναι Καναδή επιστήμονας που εξειδικεύεται στον τομέα της προστασίας των προσωπικών δεδομένων. Διατύπωσε τις επτά αρχές του "Privacy by Design" (Απόρρητο με Σχεδιασμό), οι οποίες προωθούν την ενσωμάτωση της προστασίας των δεδομένων από το στάδιο του σχεδιασμού και όλη τη διάρκεια της εφαρμογής.)
- Το πρότυπο ISO 29100: συγκατάθεση και επιλογή, σκοπός, περιορισμός συλλογής, ελάχιστοποίηση δεδομένων, περιορισμός χρήσης, ακρίβεια και ποιότητα, διαφάνεια/ενημέρωση, ατομική συμμετοχή και πρόσβαση, ευθύνη, ασφάλεια.
- Άλλες νομικές δικαιοδοσίες αναπτύσσουν επίσης νομοθεσία που επικεντρώνεται στην προστασία της ιδιωτικής ζωής. Για παράδειγμα, η Ιαπωνία ενέκρινε τον Νόμο περί Προστασίας Προσωπικών Δεδομένων που τέθηκε σε ισχύ στις 30 Μαΐου 2017.

Ο νέος νόμος δημιούργησε την Επιτροπή Προστασίας Προσωπικών Δεδομένων, επεκτείνει το πεδίο εφαρμογής και τον ορισμό του όρου "προσωπικά δεδομένα", προσθέτοντας επίσης τη νέα κατηγορία "Ευαίσθητα Προσωπικά Δεδομένα".

Βάσει του νόμου, οι φορείς πληροφοριών υποχρεούνται να λαμβάνουν τα αναγκαία και κατάλληλα μέτρα για τη διασφάλιση της ασφάλειας των προσωπικών δεδομένων. Τα μέτρα που θα θεωρηθούν κατάλληλα για την υπόθεση θα εξαρτηθούν από τη φύση, την εμβέλεια, το πλαίσιο και τον σκοπό χρήσης ή επεξεργασίας των προσωπικών δεδομένων, καθώς και από τους κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων. Σε άλλα μέρη του κόσμου, αρκετές χώρες αναπτύσσουν νομοθεσίες προστασίας προσωπικών δεδομένων. Για παράδειγμα, υπάρχει μια μη ενιαία προσέγγιση στην αφρικανική ήπειρο, όπου ορισμένες χώρες έχουν ολοκληρωμένες νομοθεσίες προστασίας προσωπικών δεδομένων και άλλες δεν έχουν νομοθεσία ή συνταγματική προστασία. Έχουν εγκρίνει νομοθεσία προστασίας δεδομένων 14 χώρες, και η Αφρικανική Ένωση έχει υιοθετήσει τη Συνθήκη της ΑΕ για την Κυβερνοασφάλεια και την Προστασία Δεδομένων, η οποία πρέπει ακόμα να τεθεί σε ισχύ. (Η συνθήκη της Αφρικανικής Ένωσης (AU Convention) αναφέρεται σε μια διεθνή συμφωνία που υιοθετήθηκε από την Αφρικανική Ένωση, η οποία αφορά την κυβερνοασφάλεια και την προστασία δεδομένων στον αφρικανικό ήπειρο.)

Επίσης, στη Νότια Αμερική, διάφορες χώρες έχουν εγκρίνει νόμους προστασίας δεδομένων: Αργεντινή, Κόστα Ρίκα, Μεξικό, Περού, Ουρουγουάη. Η Βραζιλία έχει εγκρίνει μια ολοκληρωμένη νομοθεσία προστασίας δεδομένων στις 14 Αυγούστου 2018 για την προώθηση της υιοθέτησης λύσεων IoT και την ανάπτυξη έξυπνων πόλεων στη χώρα. Ο νόμος αυτός τέθηκε σε ισχύ τον Φεβρουάριο του 2018. Κύρια χαρακτηριστικά αυτού του νέου νόμου είναι: η ίδρυση εθνικής αρχής προστασίας δεδομένων, η

εισαγωγή του αξιωματούχου προστασίας δεδομένων, η νομική βάση για την επεξεργασία δεδομένων, οι απαιτήσεις συναίνεσης, η ειδοποίηση παραβάσεων δεδομένων, η απόρριψη δεδομένων με σχετική μεταφορά.

Όπως βλέπουμε, πολλά κράτη αναπτύσσουν νόμους και κανονισμούς με στόχο την προστασία της ιδιωτικότητας των ατόμων. Η ασφάλεια των δεδομένων και οι παραβιάσεις της ιδιωτικότητας αποτελούν πραγματικά ένα από τα πιο σημαντικά προβλήματα που μπορούν να προκύψουν στις έξυπνες πόλεις. Δεδομένου ότι ο πιο σημαντικός παράγοντας στην ανάπτυξη των έξυπνων πόλεων είναι τα δεδομένα και η χρήση τους, πρέπει να είμαστε ιδιαίτερα προσεκτικοί στη διαχείρισή τους. Πράγματι, το τοπίο του IoT βασίζεται σε μεγάλο βαθμό σε προσωπικά δεδομένα για την παροχή υπηρεσιών και την αύξηση της ευημερίας των καταναλωτών, επομένως η προστασία των προσωπικών δεδομένων και η ασφάλειά τους αποτελούν κλειδί στην 'αλυσίδα δημιουργίας αξίας' του IoT. Σε αυτό το πλαίσιο, η χρήση συσκευών IoT στις έξυπνες πόλεις δεν είναι κάτι καινούργιο, αλλά καθιστά πιο περίπλοκο τον έλεγχο του υποκειμένου για τα δικά του προσωπικά δεδομένα και γίνεται πιο δύσκολο να εντοπιστούν οι νομικές βάσεις για την επεξεργασία προσωπικών δεδομένων.

Η παρουσία πολλών συσκευών, πηγών δεδομένων και οντοτήτων που επεξεργάζονται προσωπικά δεδομένα επηρεάζουν επίσης την απόκτηση της συναίνεσης του υποκειμένου για την επεξεργασία προσωπικών δεδομένων, η οποία, στο πλαίσιο των έξυπνων πόλεων, σύμφωνα με το δίκαιο της ΕΕ, μπορεί να αποτελέσει νομική βάση για την επεξεργασία προσωπικών δεδομένων των εγκαταστάσεων IoT. Υπάρχει, λοιπόν, μια άμεση σχέση μεταξύ των αρχιτεκτονικών του IoT στις έξυπνες πόλεις και της προστασίας της ιδιωτικότητας και αυτός είναι ο λόγος για τον οποίο πρέπει να προωθηθεί μια προσέγγιση της προστασίας της ιδιωτικότητας με τον σχεδιασμό.

Σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), ο οποίος πιθανώς αποτελεί τον πιο προηγμένο

νομοθετικό κανονισμό σε παγκόσμιο επίπεδο, πολλές πόλεις θα πρέπει να συμμορφωθούν με τις νομικές υποχρεώσεις λογοδοσίας στο ευρωπαϊκό δίκαιο περί προστασίας δεδομένων. Ως χειριστές δεδομένων, οι πόλεις θα υποχρεούνται να εφαρμόσουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσουν και να μπορούν να επιδείξουν ότι η επεξεργασία δεδομένων γίνεται σύμφωνα με τον GDPR, καθώς και να επανεξετάζουν και ενημερώνουν αυτά τα μέτρα όταν είναι απαραίτητο. Σε κάθε περίπτωση, οι πόλεις θα κληθούν να αξιολογήσουν ποια μέτρα θα είναι κατάλληλα. Αυτό θα εξαρτάται από τη φύση, την εμβέλεια, τα πλαίσια και τον σκοπό της επεξεργασίας, καθώς και από τους κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων. Οι ρυθμιστές σε όλο τον κόσμο επίσης υιοθετούν τον όρο της λογοδοσίας ως ένα κύριο πρότυπο στη διαχείριση διαδικασιών επεξεργασίας δεδομένων (οι ρυθμιστές προστασίας προσωπικών δεδομένων στον Καναδά, στο Χονγκ Κονγκ, στην Αυστραλία έχουν εκδώσει "Οδηγούς Λογοδοσίας" ή "Πλαισίων Διακυβέρνησης Απορρήτου" για να βοηθήσουν τον ιδιωτικό τομέα). Πρόσφατα έχουν εκπονηθεί βασικά πλαίσια για να αντιμετωπιστούν οι λύσεις IoT, επίσης στο πλαίσιο των έξυπνων πόλεων. Η συνδεσιμότητα όλων αυτών των συσκευών προϋποθέτει πολλούς κινδύνους και απαιτεί την ανάπτυξη ενός κατάλληλου νομικού πλαισίου. Το νομικό οικοσύστημα φυσικά θα ποικίλλει ανάλογα με το είδος των δραστηριοτήτων που υπάρχουν.

5.7: Προστασία Απορρήτου στις Έξυπνες Πόλεις: Επισκόπηση βασικών μέτρων

Στις έξυπνες πόλεις, η προστασία του απορρήτου αποτελεί κρίσιμη πτυχή για τη διατήρηση της ιδιωτικότητας και την εμπιστευτικότητα των πολιτών. Αυτό επιτυγχάνεται μέσω ποικίλων μέτρων και προσεγγίσεων, όπως:

1. **Ανωνυμίας Δεδομένων**: Οι έξυπνες πόλεις χρησιμοποιούν τεχνικές ανωνυμοποίησης δεδομένων για να προστατεύσουν την ταυτότητα των πολιτών, ενώ εξακολουθούν να εξάγουν χρήσιμες πληροφορίες.

2. **Ενίσχυσης της Ενημέρωσης**: Ενημέρωση των πολιτών σχετικά με τον τρόπο που συλλέγονται και χρησιμοποιούνται τα δεδομένα τους, προωθώντας τη διαφάνεια και την κατανόηση.

3. **Διαφοροποίησης Πρόσβασης**: Οριοθέτηση ποιων οντοτήτων έχουν πρόσβαση σε συγκεκριμένα είδη δεδομένων, προστατεύοντας τα πιο ευαίσθητα από παρείσφρηση.

4. **Κρυπτογράφησης Δεδομένων**: Χρήση κρυπτογράφησης για την ασφαλή αποθήκευση και μεταφορά δεδομένων, εμποδίζοντας την ανεπιθύμητη πρόσβαση.

5. **Επικαιροποίηση Νομοθεσίας**: Αναθεώρηση των νομικών πλαισίων για να ανταποκριθούν στις αλλαγές της τεχνολογίας και τις πρακτικές προστασίας του απορρήτου.

Με αυτές τις προσεγγίσεις, οι έξυπνες πόλεις διασφαλίζουν όχι μόνο την αποτελεσματική λειτουργία των ψηφιακών τους υποδομών, αλλά και τον σεβασμό της ιδιωτικής ζωής και των δικαιωμάτων των πολιτών.

Κεφάλαιο 6: Ο Ρόλος των Κυβερνήσεων σε έξυπνες πόλεις για τη διασφάλιση της ασφάλειας και της ιδιωτικότητας

Η έννοια της έξυπνης πόλης έχει εξελιχθεί σημαντικά τα τελευταία χρόνια, επιτρέποντας στις πόλεις να εκμεταλλευτούν τις σύγχρονες τεχνολογίες για να βελτιώσουν την αποτελεσματικότητα, τη βιωσιμότητα και την εμπειρία των κατοίκων. Ωστόσο, με την αύξηση των δυνατοτήτων των έξυπνων πόλεων προκύπτουν ερωτήματα σχετικά με την ασφάλεια και την ιδιωτικότητα των πολιτών. Σε αυτό το κεφάλαιο, θα εξετάσουμε τον ρόλο που διαδραματίζουν οι κυβερνήσεις στο να διασφαλίζουν την ασφάλεια και την ιδιωτικότητα σε μια έξυπνη πόλη.

6.1: Θέματα διακυβέρνησης στην επεξεργασία και διαχείριση δεδομένων

Τα δεδομένα στις εφαρμογές έξυπνων πόλεων μπορούν να αντιπροσωπεύουν τεράστιους κινδύνους ευθύνης, περιουσιακού στοιχείου, συστημικού και φήμης όσον αφορά την ασφάλεια, την ασφάλεια, την ιδιωτικότητα και άλλες πτυχές. Για παράδειγμα, η αντικατάσταση του περιεχομένου των καμερών παρακολούθησης με ψεύτικα δεδομένα ή η πρόσβαση στα προσωπικά δεδομένα υγείας ενός κατοίκου της πόλης θα μπορούσαν να προκαλέσουν σημαντικά προβλήματα σε περίπτωση παραβιάσεων δεδομένων. Παρόμοια, η διακυβέρνηση των δεδομένων μπορεί να παίξει σημαντικό ρόλο στη διευκόλυνση της επικοινωνίας, για παράδειγμα μέσω της θέσπισης κοινών προτύπων. Μπορεί επίσης να είναι σημαντική για τη δημιουργία αξίας και την αξιοποίηση της , διασαφηνίζοντας τα δικαιώματα και τις υποχρεώσεις, συμπεριλαμβανομένων των δικαιωμάτων των χρηστών ή της ιδιοκτησίας. Η ηθική της επεξεργασίας και διαχείρισης των δεδομένων είναι μια σημαντική ανησυχία στη συλλογή, επεξεργασία, εφαρμογή και αξιοποίηση των δεδομένων. Τα ηθικά ζητήματα οφείλονται στην περιορισμένη εμπιστοσύνη μεταξύ των εμπλεκομένων, τις πολύπλοκες έμμεσες σχέσεις, τις ανησυχίες για προκατάληψη στους αλγόριθμους και την ασύμμετρη πρόσβαση σε πληροφορίες και πόρους στην επεξεργασία και διαχείριση δεδομένων. Τέτοιου είδους σενάρια απαιτούν σαφείς και ευρέως υποστηριζόμενους κανονιστικούς νόμους. Υπάρχει, επομένως, ανάγκη να παρέχονται οδηγίες και διαδικασίες για τη διακυβέρνηση και διαχείριση αυτών των δεδομένων και να διευκολύνεται η

ανταλλαγή βέλτιστων πρακτικών και τεχνογνωσίας μεταξύ των πόλεων. Εφαρμόζοντας τη διακυβέρνηση της ασφάλειας και της ιδιωτικότητας των δεδομένων στις έξυπνες πόλεις, πρέπει να ληφθούν υπόψη τα ακόλουθα:

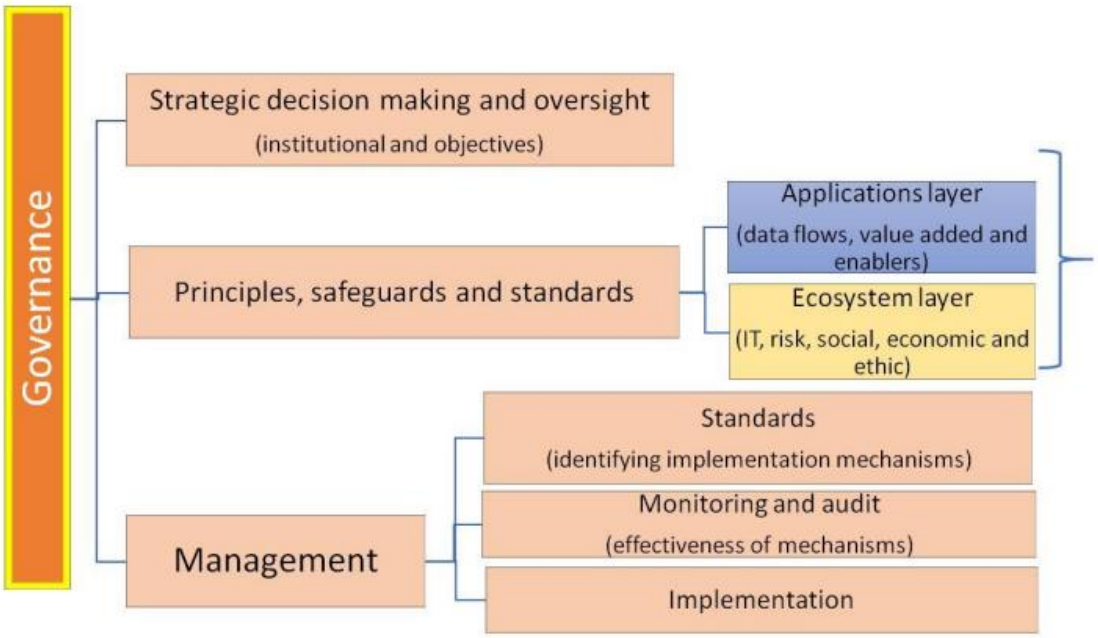
- Τα πλαισία διακυβέρνησης καθιερώνονται μέσω μιας συνδυασμένης δράσης αρμοδιοτήτων, συμπεριλαμβανομένων διεθνών συμφωνιών και πρακτικών, εθνικών κυβερνήσεων και τοπικών αυτοδιοικήσεων στις έξυπνες πόλεις.
- Η διαχείριση των δεδομένων εντός του πλαισίου διακυβέρνησης παρέχεται από ένα πολύπλοκο οικοσύστημα εμπλεκομένων φορέων (που μπορεί να περιλαμβάνει δημόσιες και ιδιωτικές οργανώσεις, καθώς και προμηθευτές).

Προς διευκόλυνση όλων μας, χρησιμοποιούμε μια ορισμένη έννοια της διακυβέρνησης που προσαρμόζεται από την UNESCO και επικεντρώνεται στην στρατηγική αρμοδιότητα λήψης αποφάσεων και στη θέσπιση δικαιωμάτων και ευθυνών. Αυτό ξεχωρίζει τη διακυβέρνηση από τη διαχείριση της επεξεργασίας και της διαχείρισης δεδομένων. Οι στόχοι για τη διακυβέρνηση δεδομένων περιλαμβάνουν, αλλά δεν περιορίζονται, τα ακόλουθα:

- Ανάπτυξη μιας κουλτούρας που βασίζεται στα δεδομένα και είναι ενημερωμένη με βάση τα στοιχεία.
- Προώθηση την ισότητας, της κοινωνική συμπερίληψης και της διαφάνειας στην οικονομία των δεδομένων.
- Ενίσχυση του προγράμματος διακυβέρνησης των δεδομένων με την υιοθέτηση ιδεών συνεργατικής καινοτομίας και ενδυνάμωσης της κοινότητας.
- Παροχή αποτελεσματικών τρόπων για τη διευκόλυνση της κατάλληλης προστασίας της απορρήτου και της ασφάλειας των δεδομένων.
- Παροχή δυνατοτήτων επιχειρηματικής ευφυούς αυτοεξυπηρέτησης.
- Υιοθέτηση κατάλληλων και αποτελεσματικών εργαλείων διαχείρισης δεδομένων.
- Αναδιαμόρφωση των ρόλων της ανάλυσης δεδομένων για την παροχή καλύτερων προβλέψεων.

Τα οφέλη ενός καλού πλαισίου διακυβέρνησης δεδομένων περιλαμβάνει τα εξής:

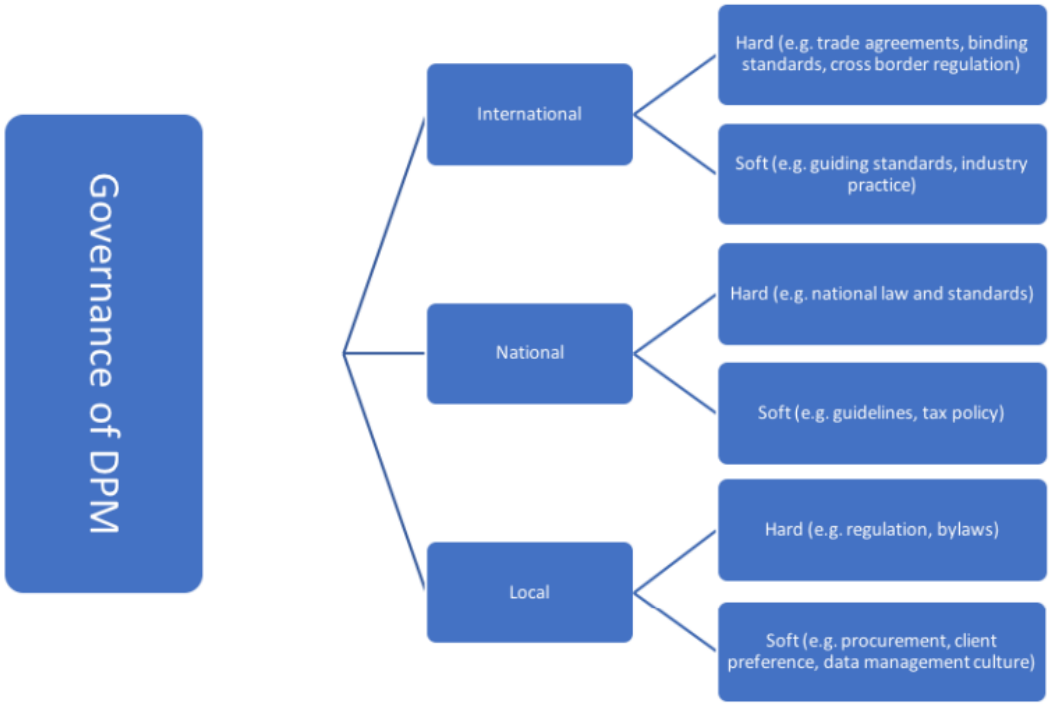
- Μείωση των δαπανών για τη δημιουργία, διατήρηση, διάθεση, αποθήκευση και χρήση των δεδομένων.
- Βελτίωση της ποιότητας των δεδομένων από πόλεις και κοινότητες, καθιστώντας τα δεδομένα αξιόπιστα, προσβάσιμα, διαθέσιμα, χρήσιμα και εντοπίσιμα.
- Διευκόλυνση της ψηφιακής συνέχειας των δεδομένων προς πληροφορίες, γνώση και έξυπνες ενέργειες.
- Ενίσχυση των εσόδων από την επεξεργασία και την εμπορευματοποίηση των δεδομένων.
- Βελτίωση της αξίας και της ποικιλίας των άμεσων και έμμεσων οφελών για τους πολίτες από την επεξεργασία και διαχείριση των δεδομένων.



Εικόνα 18 Πλαίσιο διακυβέρνησης για το DPM στο SC&C

Η Εικόνα 18 παρέχει ένα πλαίσιο για τη διακυβέρνηση της Διαχείρισης Πολιτικών Δεδομένων (ΔΠΔ) στις Τομεακές Διαδικασίες Συλλογής και Επεξεργασίας (ΤΔΣ&Ε), όπως περιγράφεται με θεματικούς όρους. Τονίζει τη διάκριση και τη σχέση μεταξύ των στοιχείων διακυβέρνησης και διαχείρισης. Το στοιχείο της

διακυβέρνησης περιλαμβάνει τη στρατηγική λήψη αποφάσεων, που θεσπίζει τα δικαιώματα και τις ευθύνες των φορέων ΔΠΔ, και τον καθορισμό υψηλού επιπέδου στόχων. Το στοιχείο της διαχείρισης περιλαμβάνει την καθημερινή εφαρμογή των συμπερασμάτων που επιτεύχθηκαν στο στοιχείο της διακυβέρνησης. Η καλή διακυβέρνηση επιτυγχάνεται μέσω της ισότητας και της συμπερίληψης στο στοιχείο της διακυβέρνησης και μέσω σαφών μηχανισμών παρακολούθησης και λογοδοσίας μεταξύ των στοιχείων διακυβέρνησης και διαχείρισης.



Εικόνα 19 Πλαίσιο δικαιοδοσίας για τη διακυβέρνηση του DPM στο SC&C

Η Εικόνα 19 περιγράφει την ποικιλομορφία των γεωγραφικών ή δικαιοδοτικών εισροών σε ένα πλαίσιο διακυβέρνησης.

Κανένας φορέας, είτε δημόσιος είτε ιδιωτικός, δεν είναι πραγματικά ανεξάρτητος στη διακυβέρνηση των ΔΙΔ (Data Privacy Management) για τις Έξυπνες Πόλεις και Κοινότητες. Κάθε φορέας πρέπει να χαρτογραφήσει και να λάβει υπόψη τις δεσμευτικές υποχρεώσεις και επιρροές που ισχύουν για τη συγκεκριμένη δραστηριότητά του και τον ευρύτερο πλαίσιο. Στις καλά ανεπτυγμένες αγορές, οι τοπικές και εθνικές εισροές σε ένα πλαίσιο διακυβέρνησης συνήθως είναι σχετικά καλά κατανοητές και εύκολα αναγνωρίσιμες, ακόμα κι αν είναι μερικές φορές πολύπλοκες. Οι διεθνείς εισροές είναι συχνά πιο προβληματικές, όχι μόνο λόγω της διασυνοριακής φύσης πολλών δραστηριοτήτων ΔΙΔ, ακόμα και όταν επικεντρώνονται σε Έξυπνες Πόλεις και Κοινότητες. Για παράδειγμα, πολλά συστήματα βασισμένα στον νέφος (cloud) μπορεί να εξαρτώνται από τη χρήση διακομιστών σε πολλαπλές τοποθεσίες και αυτό μπορεί να καθιστά μια δραστηριότητα υποκείμενη στους νόμους περισσότερων από ένα κράτη. Επίσης, ορισμένες κανονιστικές προσεγγίσεις για την προστασία του απορρήτου επικεντρώνονται στη νομική θέση του ατόμου και όχι στην τοποθεσία μιας συναλλαγής και, συνεπώς, μπορεί να καθιστούν την εντοπισμό του ισχύοντος δικαίου πιο προβληματικό.

6.2: Πλαίσιο διακυβέρνησης για την επεξεργασία και διαχείριση δεδομένων

6.2.1: Οι βασικές αρχές για την διακυβέρνηση δεδομένων

Τα τρία θεμέλια της διακυβέρνησης δεδομένων είναι:

1) Οι κανόνες και οι πολιτικές που θα επιτρέπουν σε ένα έξυπνο δημοτικό σώμα ή εθνική αρχή να επιβλέπει τις δραστηριότητες που σχετίζονται με τη Διαχείριση Δεδομένων Πόλης (ΔΔΠ), δηλαδή να αποκτά μια συνολική εικόνα της δραστηριότητάς της και, κατ' επέκταση, των σχετικών δεδομένων.
    - Μια έξυπνη πόλη θα πρέπει να είναι σε θέση να αποτυπώνει την συνολική εικόνα της δραστηριότητάς της και θα πρέπει επίσης να είναι σε θέση να αποτυπώνει την εικόνα των δεδομένων που ανήκουν, χρησιμοποιούνται και αποθηκεύονται εντός του οικοσυστήματος.
    - Η εικόνα θα πρέπει να αποτυπώνει με ακρίβεια τη δραστηριότητα. Οι οργανισμοί του οικοσυστήματος που εμπλέκονται στην επεξεργασία δεδομένων θα πρέπει να διευκολύνουν τις δυνατότητες συγκέντρωσης δεδομένων και τις πρακτικές αναφοράς προκειμένου να ενισχυθεί η παρακολούθηση της δραστηριότητας και των κινδύνων, η επιτήρηση και η δυνατότητα αναγνώρισης και παρακολούθησης προβλημάτων με γρήγορο τρόπο.
    - Η διαχείριση των δεδομένων απαιτεί ευελιξία, η οποία παρέχεται από ευέλικτα εργαλεία που πρέπει να σχεδιαστούν με σαφή σκοπό. Ωστόσο, συμβαίνει να μην είναι γνωστό το τελικό μοντέλο επειδή πρόκειται για μια νέα δραστηριότητα ή έναν νέο τομέα, όπως οι επιχειρήσεις IoT και έξυπνες πόλεις. Μέχρι να γίνει γνωστό το τελικό μοντέλο, δεν είναι δυνατό να σχεδιαστούν ειδικά εργαλεία και πρέπει να συλλεγούν λεπτομερή δεδομένα για να διατηρηθεί η μέγιστη ευελιξία.

2) Κανόνες και πολιτικές περί ποιότητας δεδομένων

- Κάθε οργάνωση πρέπει να είναι σε θέση να ταξινομεί τα δεδομένα και να αναγνωρίζει εάν τα δεδομένα είναι κρίσιμα για την οργάνωση ή όχι.
- Τα κρίσιμα δεδομένα πρέπει πάντα να προστατεύονται, να ενημερώνονται και να γίνεται ότι είναι απαραίτητο για να διατηρηθεί η υψηλότερη δυνατή ποιότητά τους με την πάροδο του χρόνου.
- Η ποιότητα των δεδομένων υψηλής αξίας πρέπει να παρακολουθείται σε τακτική βάση και πρέπει να αποτελεί υπόθεση όλων στο Οικοσύστημα.
- Η ποιότητα των δεδομένων είναι πάντα το αποτέλεσμα μιας συνεχούς προσπάθειας.
- Κάθε είδος δεδομένων πρέπει να χαρακτηρίζεται από έναν κύκλο ζωής, επιτρέποντας την εφαρμογή κατάλληλων κανόνων (π.χ. διαγραφή δεδομένων).
- Τα επαναλαμβανόμενα, ασήμαντα ή παρωχημένα (ROT) δεδομένα δεν πρέπει να αποθηκεύονται και πρέπει να διαγράφονται για να περιοριστεί η σπατάλη πόρων που συνδέεται με την αποθήκευση, την ασφάλεια, την επεξεργασία και την εξόρυξη δεδομένων.

3) Οι κανόνες και οι πολιτικές για τους χρήστες και τους παρόχους δεδομένων, καθώς και η βελτίωση της χρησιμότητας και της καταγωγής των δεδομένων μέσω εργαλείων διαχείρισης καταγωγής, απαιτούν:
    - "Δεδομένα που είναι κατάλληλα για χρήση" απαιτούν επικοινωνία μεταξύ χρηστών και παρόχων.
    - Τα κύρια εμπόδια στην επικοινωνία μεταξύ χρηστών και παρόχων είναι:
        - Τα άτομα και/ή οι πάροχοι δεν είναι σαφώς αναγνωρισμένοι.
        - υπάρχει χρονική καθυστέρηση μεταξύ της παραγωγής και της χρήσης δεδομένων: τα δεδομένα χρησιμοποιούνται αρκετούς μήνες ή χρόνια μετά την παραγωγή.

    - Για να βελτιωθεί η επικοινωνία, χρησιμοποιούνται εργαλεία που βελτιώνουν τη «χρηστικότητα» και την καταγωγή των δεδομένων.

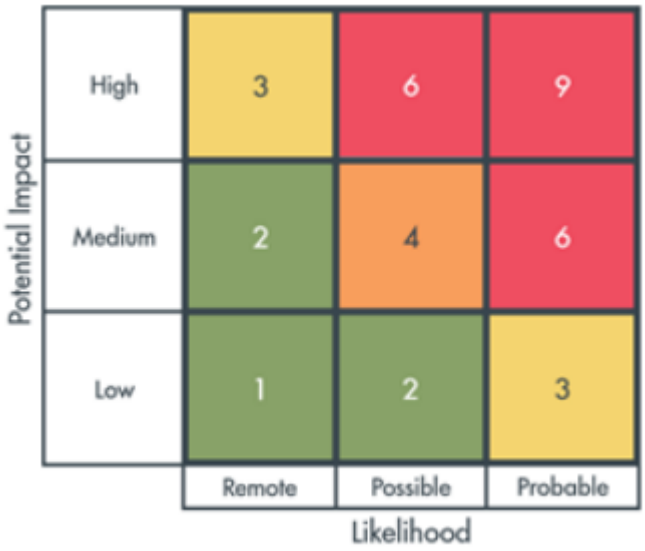
        Αυτά τα εργαλεία είναι:
        - Η χρήση ενός κοινού γλωσσικού κώδικα
        - Η διαθεσιμότητα μιας ευανάγνωστης τεκμηρίωσης, περιλαμβανομένων ορισμών και μεθοδολογιών υπολογισμού εάν υπάρχουν, που εφαρμόζονται στα δεδομένα.
        - Ετικέτες για κάθε δεδομένο.
        - Μεταδεδομένα.

    - Η σημασία της καταγωγής και η χρησιμότητα των δεδομένων πρέπει να είναι γνωστή και κατανοητή από κάθε πάροχο και χρήστη.
    - Η διακυβέρνηση πρέπει να προωθεί το "Πολιτισμός Ποιότητας Δεδομένων". Αυτό σημαίνει ότι η διακυβέρνηση πρέπει να ενθαρρύνει μια πολιτιστική προσέγγιση προς την ποιότητα

των δεδομένων. Αυτό συμπεριλαμβάνει την υποστήριξη πρακτικών και διαδικασιών που επιδιώκουν τη βελτίωση της ποιότητας των δεδομένων και την προαγωγή μιας κουλτούρας όπου η προσοχή στην ποιότητα είναι βασική αξία.

6.2.2: Η σχέση μεταξύ ασφάλειας, ιδιωτικότητας και διακυβέρνησης

Η σχέση μεταξύ ασφάλειας και ιδιωτικότητας φαίνεται στην εικόνα 20.



Εικόνα 20 Κλίμακα αξιολόγησης επιχειρηματικού κινδύνου,

πηγή : CGMA (Chartered Global Management Accountant) Ιανουάριος

Στο πρώτο παράδειγμα, το Coso* προτείνει την εφαρμογή μιας μεθοδολογίας που ονομάζεται Heat Map40, όπως φαίνεται στο ακόλουθο απλό παράδειγμα (Εικόνα 20), όπου οι συνέπειες (εδώ ονομάζονται πιθανές επιπτώσεις) και η πιθανότητα , κατατάσσονται σύμφωνα με το επίπεδο κινδύνου.

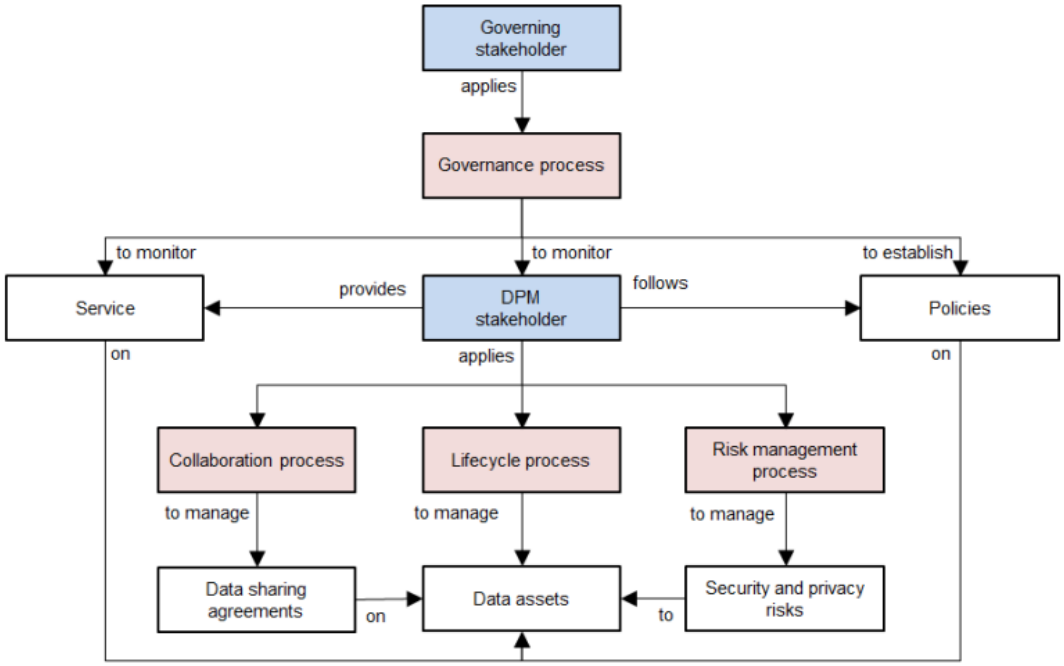
*Το COSO είναι ένα ακρώνυμο που αναφέρεται στην Επιτροπή Ενδοεπιχειρησιακού Ελέγχου Οργανισμών (Committee of Sponsoring Organizations of the Treadway Commission).

- Ένας κυβερνών εφαρμόζει ένα διακυβερνητικό πλάνο στο οικοσύστημα:
    - για να θεσπίσει πολιτικές,
    - για να παρακολουθεί έναν ενδιαφερόμενο στη διαχείριση επεξεργασίας δεδομένων (DPM) που παρέχει υπηρεσίες σε δεδομένα.
    - για να παρακολουθεί υπηρεσίες σε λειτουργία.

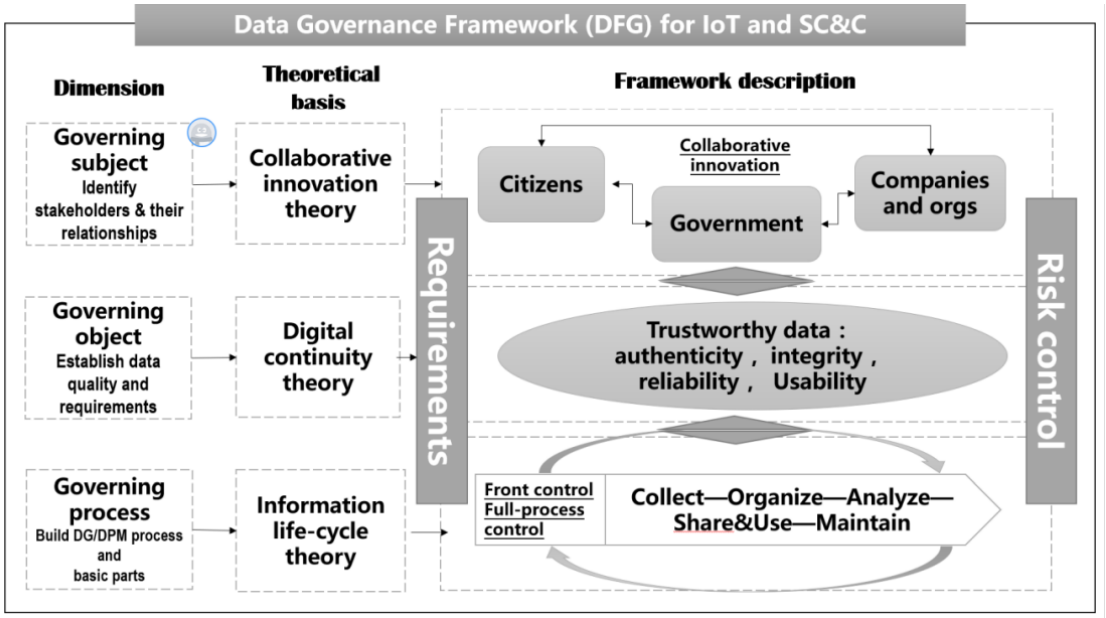
Μια οντότητα μπορεί να είναι ένα άτομο, ένα σύστημα, μια οργάνωση.

- Ένας ενδιαφερόμενος στη διαχείριση επεξεργασίας δεδομένων παρέχει μια υπηρεσία σε δεδομένα, ακολουθώντας πολιτικές.
- Ένας ενδιαφερόμενος στη διαχείριση επεξεργασίας δεδομένων εφαρμόζει τις ακόλουθες διαδικασίες:
    - Ένα διαδικαστικό πλαίσιο συνεργασίας για τη διαχείριση των συμφωνιών κοινής χρήσης δεδομένων μεταξύ ενδιαφερομένων στο οικοσύστημα.
    - Ένα διαδικαστικό πλαίσιο κύκλου ζωής για τη διαχείριση των δεδομένων που χρησιμοποιούνται και ενημερώνονται από την υπηρεσία, σύμφωνα με τις πολιτικές που έχει θεσπίσει ο κυβερνών φορέας.
    - Και ένα διαδικαστικό πλαίσιο διαχείρισης κινδύνων για τη διαχείριση των κινδύνων ασφάλειας και ιδιωτικότητας στα δεδομένα.

Όλα τα παραπάνω φαίνονται στην ακόλουθη εικόνα:



Εικόνα 21 Ασφάλεια σχέσεων, απόρρητο και διακυβέρνηση στο DPM (Data Privacy Managment)



Εικόνα 22 Βασικά στοιχεία ενός πλαισίου διακυβέρνησης δεδομένων

Η εικόνα 22 περιγράφει τα στοιχεία ενός πλαισίου διακυβέρνησης δεδομένων για το Διαδίκτυο των Πραγμάτων (IoT) και τον Εφοδιαστικό Έλεγχο και Εντοπισμό (SC&C) βασισμένο σε τρεις κύριες διαστάσεις:

a. Η διάσταση του διακυβερνούμενου θέματος που παρέχει ένα σχέδιο συμμετοχής,
b. Η διάσταση του διακυβερνούμενου αντικειμένου που παρέχει ένα σχέδιο δεδομένων, και
c. Η διάσταση της διακυβέρνησης διαδικασίας που παρέχει ένα σχέδιο διαδικασίας και διαχείρισης δεδομένων.

Κεφάλαιο 7: Συμπεράσματα

Στο πλαίσιο αυτής της εργασίας, εξετάσαμε προσεκτικά την έννοια των Έξυπνων Πόλεων, εστιάζοντας ιδιαίτερα στην προστασία της ιδιωτικότητας και την ενίσχυση της ασφάλειας των πολιτών. Μέσω μιας εκτενούς μελέτης και ανάλυσης των τεχνολογιών και των πρακτικών που εφαρμόζονται σε παγκόσμιο επίπεδο, καταλήξαμε σε σημαντικά συμπεράσματα.

Αρχικά, αναγνωρίσαμε την κρίσιμη σημασία της διασφάλισης της ιδιωτικότητας των πολιτών σε μια Έξυπνη Πόλη. Η εφαρμογή τεχνολογιών πρέπει να γίνεται με σεβασμό προς την προσωπική ζωή και τα δικαιώματα των ατόμων, αποφεύγοντας την υπερβολική συλλογή και χρήση προσωπικών δεδομένων.

Επιπλέον, προτείνουμε την ενίσχυση των μέτρων ασφαλείας σε όλα τα επίπεδα, από την προστασία των υποδομών έως την εκπαίδευση των πολιτών για την ασφαλή χρήση των τεχνολογιών. Η αποτελεσματική εφαρμογή αυτών των μέτρων θα βοηθήσει στην αντιμετώπιση πιθανών κινδύνων ασφαλείας και στη δημιουργία ενός περιβάλλοντος που ενθαρρύνει την ελεύθερη και ασφαλή συμμετοχή των πολιτών.

Τέλος, ενθαρρύνουμε την συνεχή έρευνα και ανάπτυξη σε αυτό τον τομέα, προκειμένου να εξελιχθούν οι τεχνολογίες και οι πρακτικές με σκοπό την ακόμη μεγαλύτερη προστασία της ιδιωτικότητας και την ενίσχυση της ασφάλειας στις Έξυπνες Πόλεις. Μόνο μέσα από τη συνεχή προσπάθεια και τη συνεργασία μεταξύ κυβερνήσεων, επιχειρήσεων και κοινοτήτων μπορούμε να επιτύχουμε ένα βιώσιμο και ασφαλές μέλλον για τις πόλεις μας.

Βιβλιογραφία

1. Mahmoud AL-HADER and Ahmad RODZI , "*THE SMART CITY INFRASTRUCTURE DEVELOPMENT & MONITORING"*

2. Ayoub Arroub, Bassma Zahi, Mohamed Sadik, Essaid Sabir , *"A literature review on Smart Cities: Paradigms, opportunities and open problems"*

3. Sarah Burch , "*Accelerating a Just Transition to Smart, Sustainable Cities*"

4. ROBERT J. BUTLER and IRVING LACHOW , "*Smart Cities and the Internet of Things: Benefits, Risks, and Options*"

5. Keyur K Patel , Sunil M Patel - PG Scholar Assistant Professor – *"Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges"*

6. Kaivan Karimi , Gary Atkinson , "*What the Internet of Things (IoT) Needs to Become a Reality"*

7. Chai K. Toh *, "Security for smart cities"*

8. Office Of The Victorian Information Commissioner ,*"The Internet of Things and privacy"*

9. Strategic Studies Institute, US Army War College , Nir Kshetri , "*CYBERSECURITY AND PRIVACY ISSUES FACING SMART CITIES*"

10. Bernard Cathelat , UNESCO , "*SMART CITIES SHAPING THE SOCIETY OF 2030*"

11. Robert Lewis-Lettington, Pasquale Annicchino, Nathalie Feingold, Antonio Kung , Gyu Myoung Lee - *"Framework for security, privacy, risk and governance in data processing and management"*

12. Mohammad Hosein Panahi Rizi , Dr. Seyed Amin Hoseini Seno , *"A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city"*

13. Natasha Cohen and Brian Nussbaum , *"What is a Smart City?"*

14. Abbas Shah Syed, Daniel Sierra-Sosa, Anup Kumar and Adel Elmaghraby *, "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges"*

15. Soumyalatha, Shruti G Hegde , *"Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges"*

16. https://www.lifo.gr/now/tech-science/barkeloni-i-pio-exypni-poli-toy-kosmoy

17. https://www.citybranding.gr/2014/04/blog-post_10.html

18. *https://gr.euronews.com/business/2015/05/25/smarter-living-in-barcelona*

19. *https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_el*

20. *https://smartcity.heraklion.gr/el/home/*

21. *https://eleftheriaonline.gr/local/politiki/aftodioikisi/dimoi/item/263721-kalamata-ksekinise-i-egkatastasi-27-eksypnon-staseon-astikis-sygkoinonias*

22. *https://www.kalamata.gr/el/enimerosi/news/22369-ksekinise-i-egkatastasi-eksypnon-staseon-stin-kalamata*

23. *https://www.in.gr/2021/11/15/stories/seoul-mia-eksypni-poli-ton-10-lepton/*

24. *https://www.iefimerida.gr/kosmos/seoyl-sto-fos-shedia-gia-dimioyrgia-polis-ton-10-lepton*

25. *https://www.lifo.gr/now/world/project-h1-geitonia-tis-seoyl-metamorfonetai-se-10lepti-poli-horis-ihnos-aytokinitoy*

26. *https://www.lifo.gr/now/perivallon/i-sigkapoyri-kataskeyazei-oikologiki-exypni-poli-me-42000-katoikies*

27. *https://www.mononews.gr/agores/think-tanks/giati-i-sigkapouri-ine-i-pio-exipni-poli-tou-kosmou*

28. *https://www.kathimerini.gr/opinion/902207/h-exypni-poli-ton-trikalon-kai-to-mellon-tis-elladas/*

29. *https://www.protothema.gr/technology/article/692194/i-halkida-apektise-efarmoges-smart-city/*